Nations Unies A/75/123

Assemblée générale

Distr. générale
23 juin 2020
Français
Original :anglais/arabe/espagnol/
français

Soixante-quinzième session
Point 98 de la liste préliminaire*

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/75/50.

20-08285 (F) 100820 180820

I. Introduction

1. Le 12 décembre 2019, l'Assemblée générale a adopté la résolution 74/28, intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » au titre du point 93 de l'ordre du jour relatif aux progrès de l'informatique et des télécommunications et à la sécurité internationale.

2. Au paragraphe 2 de la résolution 74/28, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, leurs vues et observations sur les questions suivantes :

a) les efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine ;

b) la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

3. Comme suite à cette demande, le 27 janvier 2020, une note verbale a été envoyée aux États Membres pour les inviter à communiquer des informations à ce sujet. En raison de la crise actuelle liée à la maladie à coronavirus (COVID-19) et afin que les États Membres puissent plus facilement soumettre leurs vues sur les questions ci-dessus, la date butoir, initialement fixée au 15 mai 2020, a été reportée au 31 mai 2020.

4. Les réponses reçues au moment de l'établissement du présent rapport sont reproduites dans les sections II et III ci-dessous. Les réponses reçues après le 31 mai 2020 seront publiées dans la langue dans laquelle elles ont été présentées sur le site Web du Bureau des affaires de désarmement (https://www.un.org/disarmament/fr/informatique-et-telematique/).

II. Réponses reçues des gouvernements

Arménie

[Original : anglais]
[13 mai 2020]

L'Arménie attache une grande importance à un cyberespace ouvert, libre, stable, sûr et conforme aux normes et principes du droit international et à la Charte des Nations Unies dans leur ensemble. Étant donné le caractère mondial du cyberespace, il est important de protéger les droits de la personne et les libertés fondamentales en ligne, en particulier la liberté d'opinion et d'expression, qui inclut le droit de rechercher, de recevoir et de diffuser des informations. Par ailleurs, les difficultés émanant de l'utilisation des technologies numériques et de l'environnement numérique sont diverses et variées. La communauté internationale devrait donc faire front commun afin de prévenir toute utilisation abusive des technologies numériques et contribuer à leur utilisation pacifique dans un esprit de coopération. À cette fin, l'Arménie participe activement aux plateformes internationales de coopération visant à accroître la transparence, la prévisibilité et la stabilité du cyberespace et à réduire les risques de menaces émanant de l'utilisation des technologies numériques.

L'Arménie est fortement attachée à la pleine mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité et de son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes

informatiques. Depuis 2019, elle participe activement à l'exécution du projet CyberEast, un projet conjoint de l'Union européenne et du Conseil de l'Europe dont le but est d'assurer le renforcement des capacités en ce qui concerne la cyberrésilience, la justice pénale et les preuves électroniques. De même, elle met en œuvre de bonne foi les mesures de confiance de l'Organisation pour la sécurité et la coopération en Europe (OSCE) (décision du Conseil permanent 1202) afin d'atténuer les menaces émanant de l'utilisation des technologies numériques. En juillet 2019, l'Arménie a accueilli une équipe d'experts du Département des menaces transnationales de l'OSCE afin de procéder à une évaluation de ses capacités nationales en matière d'enquêtes et de poursuites judiciaires dans le domaine de la cybercriminalité. En novembre 2019, le Département a organisé une table ronde conjointe à Erevan afin de discuter avec les parties prenantes arméniennes des conclusions de ladite évaluation. Sur la base du rapport d'évaluation des experts et des conclusions de la réunion de table ronde, il a élaboré une note de cadrage consacrée à ce sujet, qui pourrait servir de base à un futur projet.

Le contenu des rapports de 2013 et de 2015 du Groupe d'experts gouvernementaux et les conclusions qui en émanent ne reflètent que le point de vue d'un nombre limité d'États Membres de l'ONU ayant participé à l'élaboration de ces rapports. En tant que tels, ils n'ont par conséquent pas contribué à la création d'un ensemble universel et exhaustif de normes acceptables par tous les États Membres. L'Arménie estime donc que, en tant que plateforme inclusive et transparente de discussion entre États Membres, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale pourrait élaborer une liste récapitulative complète des règles, normes et principes de comportement responsable des États pour l'utilisation des technologies numériques que tous les États Membres pourraient accepter.

Australie

[Original : anglais]
[29 mai 2020]

L'Australie se félicite de l'occasion qui lui est donnée de présenter, en réponse à l'invitation formulée dans la résolution 74/28 de l'Assemblée générale, ses vues sur la promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. La présente communication se fonde sur les informations transmises par l'Australie en réponse aux résolutions 70/237, 68/243 et 65/41 sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en 2016, 2014 et 2011 respectivement.

Dans ses rapports de 2010 (A/65/201), de 2013 (A/68/98) et de 2015 (A/70/174), le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale affirme que le droit international existant, et en particulier la Charte des Nations Unies dans son intégralité, est applicable et essentiel au maintien de la paix et de la stabilité et à la mise en place d'un environnement informatique ouvert, sûr, stable, accessible et pacifique. Ces rapports énoncent également des normes facultatives et non contraignantes de comportement responsable des États tout en mettant en exergue l'importance de mesures de confiance et d'activités coordonnées de renforcement des capacités. Ensemble, ces mesures (le droit international, les normes, les mesures de confiance et le renforcement des capacités) jettent les bases d'un cyberespace sûr, stable et prospère et sont souvent qualifiées de cadre de comportement responsable des États.

L'Australie réaffirme l'engagement qu'elle a pris de se conformer aux rapports du Groupe d'experts de 2010, 2013 et 2015 (A/65/201, A/68/98 et A/70/174). Elle participe activement aux travaux du sixième Groupe d'experts et à ceux de la session inaugurale du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (créés en vertu des résolutions 73/266 et 73/27 respectivement).

Droit international

La position de l'Australie sur la manière dont le droit international régit la conduite des États dans le cyberespace est énoncée dans la Stratégie internationale d'engagement informatique de 2017, complétée par le Supplément de 2019 sur le droit international (tous deux accessibles sur le site Web du Département australien des affaires étrangères et du commerce : https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf).

En février 2020, l'Australie a publié un document interne intitulé « Études de cas sur l'application du droit international dans le cyberespace ». Il est disponible sur le site Web du Groupe de travail à composition non limitée (https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf) et sur le site Web du Département australien des affaires étrangères et du commerce (www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf).

Application

Rappelant que, en 2015, l'Assemblée générale a demandé à tous les États Membres de l'ONU « de s'inspirer, pour ce qui touche à l'utilisation de l'informatique et des technologies des communications, du rapport de 2015 du Groupe d'experts gouvernementaux » (voir résolution 70/237), l'Australie a publié un aperçu de la manière dont elle respecte et met en œuvre les quatre piliers dudit rapport : le droit international, les normes de comportement responsable des États, les mesures de confiance et le renforcement des capacités. Cet aperçu est disponible sur le site Web du Groupe de travail à composition non limitée (https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf) et sur celui du Département australien des affaires étrangères et du commerce (https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace).

Dans son rapport de 2015, le Groupe d'experts gouvernementaux a présenté les meilleures pratiques, que nombre d'États appliquaient ou appliquent déjà. L'Australie encourage tous les pays à dresser le bilan de leurs activités qui s'inscrivent dans le droit fil du rapport de 2015 du Groupe d'experts gouvernementaux (application du droit international, application de normes de comportement responsable des États, mesures de confiance et renforcement des capacités) et à recenser les lacunes ainsi que les capacités nécessaires pour combler celles-ci, le cas échéant. Avec le concours du Mexique et de 24 autres pays, elle a eu le plaisir de soumettre au Groupe de travail à composition non limitée (créé en vertu de la Résolution 73/27 de l'Assemblée générale) une proposition visant à organiser une *Enquête sur la mise en œuvre au niveau national de la résolution 70/237 de l'Assemblée générale*. Cette proposition est disponible sur le site Web du Groupe de travail (https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf) ainsi que sur celui du Département australien des affaires étrangères et du commerce (https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf).

Genre

Comme indiqué dans le programme pour les femmes et la paix et la sécurité, les conflits et les menaces contre la paix et la sécurité internationales ont des répercussions uniques et différentes sur les femmes. L'Australie félicite l'Institut des Nations Unies pour la recherche sur le désarmement pour son récent rapport intitulé « Still behind the curve: gender balance in arms control, non-proliferation and disarmament diplomacy » (Une évolution lente : la représentation équilibrée des genres et la diplomatie de la maîtrise des armements, de la non-prolifération et du désarmement). Le rapport indique que, parmi les Grandes commissions de l'Assemblée générale, c'est à la Première Commission que l'on trouve la plus faible proportion de femmes diplomates. Le Women in International Security and Cyberspace Fellowship est une initiative conjointe des Gouvernements australien, britannique, canadien, néerlandais et néo-zélandais, visant à promouvoir une plus large participation des femmes aux discussions qui ont trait à la sécurité internationale et au comportement responsable des États dans le cyberespace et qui se tiennent à l'Organisation des Nations Unies. L'Australie continuera de promouvoir par le biais de mesures concrètes la participation active et effective des femmes aux discussions multilatérales relatives à la sécurité internationale et au désarmement.

Bosnie-Herzégovine

[Original : anglais]
[11 mai 2020]

Informations sur les efforts engagés au niveau national en Bosnie-Herzégovine pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

Le présent rapport a été élaboré sur la base de données recueillies par les institutions de Bosnie-Herzégovine suivantes : Ministère de la sécurité de Bosnie-Herzégovine, Ministère de la défense de Bosnie-Herzégovine, Ministère des transports et des communications de Bosnie-Herzégovine, Administration fédérale de police, Ministère de l'intérieur de la Republika Srpska et Ministère du développement scientifique et technologique, de l'enseignement supérieur et de la société de l'information de la Republika Srpska. Les institutions compétentes suivantes n'avaient pas transmis les données pertinentes au Ministère de la sécurité de Bosnie-Herzégovine avant l'envoi du présent rapport : Police du District de Brcko et Ministère fédéral du transport et des communications.

La Bosnie-Herzégovine a signé différents traités et conventions internationaux relatifs à l'information et à la cybersécurité, notamment la Convention sur la cybercriminalité et l'Accord d'association et de stabilisation. La Convention a été ouverte à la signature le 23 novembre 2001 à Budapest tandis que la Présidence de la Bosnie-Herzégovine a pris la décision de la ratifier à sa 89e session, le 25 mars 2006. La Bosnie-Herzégovine s'est ainsi engagée à adopter des lois et toute autre mesure nécessaire pour lutter contre la cybercriminalité et à les harmoniser avec celles des autres signataires de la Convention, notamment en ce qui concerne les poursuites pénales, ainsi que l'acquisition, le traitement et le stockage des données.

Eu égard aux questions couvertes par la Convention, la Bosnie-Herzégovine a adopté les lois suivantes :

- Code pénal de Bosnie-Herzégovine, Journal officiel de Bosnie-Herzégovine, no 3/03 ;

- Code de procédure pénale, Journal officiel de Bosnie-Herzégovine, nos 3/03, 32/03, 36/03, 26/04,63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13 ;
- Code pénal de la Fédération de Bosnie-Herzégovine, Journal officiel de la Fédération de Bosnie-Herzégovine, nos 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 et 75/17 ;
- Code de procédure pénale de la Fédération de Bosnie-Herzégovine, Journal officiel de la Fédération de Bosnie-Herzégovine, nos 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13, 59/14 ;
- Code pénal de la Republika Srpska, Journal officiel de la Republika Srpska, nos 64/17 et 104/18 ;
- Code de procédure pénale de la Republika Srpska, Journal officiel de la Republika Srpska, nos 53/12, 91/17 et 66/18 ;
- Code pénal du District de Brcko, Journal officiel du District de Brcko, nos 33/13, 26/16, 13/17 et 50/18 ;
- Code de procédure pénale du District de Brcko, Journal officiel du District de Brcko, nos 33/13, 27/14, et 3/19 ;

Au niveau de l'État

Encouragé par ce qui précède et conscient des risques pouvant subvenir dans le cyberespace, le Ministère de la sécurité de Bosnie-Herzégovine a entrepris les activités suivantes.

À l'initiative du Ministère de la sécurité de Bosnie-Herzégovine, le Conseil des ministres a adopté, à sa quatre-vingt-treizième session, le 8 mars 2017, la Décision portant création de l'équipe d'intervention en cas d'atteinte à la sécurité informatique pour les institutions de Bosnie-Herzégovine. Cette décision, qui porte création de l'équipe d'intervention et la subordonne au Département de l'informatique et des télécommunications du Ministère de la sécurité de Bosnie-Herzégovine, a été publiée au Journal officiel de Bosnie-Herzégovine no 25/17.

En vertu de l'article 4 de ladite décision, le Ministère de la sécurité doit adapter son organisation interne et institutionnaliser des postes afin d'assurer le bon fonctionnement de l'équipe d'intervention. Conformément aux procédures relatives à la modification de la structure interne et à la systématisation institutionnelle, l'avis des institutions concernées a été sollicité. Leur réponse, reçue fin 2017, a été positive et les documents nécessaires ont tous été établis.

Le Ministère de la sécurité de Bosnie-Herzégovine a apporté les modifications nécessaires à sa structure interne et institutionnalisé des postes de sorte à assurer le bon fonctionnement de l'équipe d'intervention. La décision a ensuite été transmise au Conseil des ministres pour adoption. L'approbation d'un manuel proposé au Conseil des ministres est pour le moment en attente. Une fois le manuel approuvé, le Ministère de la sécurité de Bosnie-Herzégovine se penchera sur les aspects techniques et opérationnels de la création d'une équipe d'intervention en cas d'atteinte à la sécurité informatique pour les institutions nationales.

Les modifications proposées à la structure interne incluent la création de cinq postes supplémentaires au sein d'une nouvelle division subordonnée au Département de l'informatique et des télécommunications.

Le Ministère de la sécurité prévoit de renforcer l'équipe d'intervention sur le plan opérationnel, institutionnel et technique de sorte qu'elle puisse atteindre ses

objectifs stratégiques (assurer la coordination et la coopération entre les organismes compétents de Bosnie-Herzégovine ; éliminer et atténuer les conséquences d'atteintes à la sécurité causées par un accès non autorisé aux systèmes informatiques des institutions bosniennes ; renforcer la fiabilité des systèmes informatiques des institutions bosniennes par le biais d'un travail continu et de la prévention et de la réduction des atteintes à la sécurité ; aider le personnel administratif à répondre à de tels incidents, etc.), mener les activités prévues par l'article 6 de la Décision et créer un réseau d'équipes d'intervention en cas d'atteinte à la sécurité informatique en Bosnie-Herzégovine.

En outre, à l'initiative du Ministère de la sécurité, le Conseil des ministres a adopté, à sa cent-septième session, le 6 juillet 2017, l'analyse sur l'harmonisation de la législation dans le domaine de la cybersécurité. Il a également exhorté le Ministère de la sécurité à redoubler d'efforts pour élaborer une stratégie de cybersécurité en Bosnie-Herzégovine.

Les organismes pertinents sont par conséquent en train d'harmoniser leur position en ce qui concerne le modèle de la stratégie. Ce modèle sera mis en conformité avec la Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et avec les dispositions constitutionnelles nationales.

Un Groupe de travail informel a été mis sur pied sous les auspices de l'Organisation pour la coopération et la sécurité en Europe. Il rassemble des représentants des institutions bosniennes compétentes et intéressées et a rédigé les Lignes directrices pour le cadre stratégique de cybersécurité en Bosnie-Herzégovine.

Le Ministère de la sécurité participe aussi actuellement à la rédaction de la nouvelle stratégie bosnienne pour la prévention du terrorisme et la lutte contre celui-ci, qui devrait inclure la problématique de l'utilisation de l'environnement numérique à des fins terroristes.

Le Ministère participe en outre activement aux travaux du Comité de la Convention du Conseil de l'Europe sur la cybercriminalité.

À l'initiative du Ministère de la sécurité, le Conseil des ministres a adopté, à sa quatre-vingtième session, le 10 novembre 2016, la Décision relative à la création d'un groupe de travail interministériel pour l'exécution d'un projet de renforcement des capacités dans le domaine de la cybercriminalité (projet iPROCEEDS). Cette décision a été publiée au Journal officiel de Bosnie-Herzégovine nº 14/17.

En janvier 2016, l'Union européenne et le Conseil de l'Europe ont signé un accord sur un projet régional baptisé iPROCEEDS visant à renforcer les capacités des pays d'Europe du Sud-Est à lutter contre la cybercriminalité. Dans le cadre de ce projet, dont la durée est de quarante-deux mois, l'accent sera mis sur la confiscation des produits de la criminalité sur Internet et de la cybercriminalité. Le projet a été financé par l'Union européenne et le Conseil de l'Europe, tandis que le Bureau de la cybercriminalité du Conseil, dont le siège se trouve à Bucarest, est responsable de sa mise en œuvre. Il a été proposé que l'équipe de projet représentant la Bosnie-Herzégovine soit composée de représentants des organismes compétents en matière de cybercriminalité, à savoir le Ministère de la justice, le Parquet, la police, le Département du renseignement financier et d'autres. Conformément à cette proposition, un groupe de travail a été mis sur pied.

En outre, le Ministère de la sécurité de Bosnie-Herzégovine assure la coordination entre les membres de l'équipe de projet dans le cadre de iPROCEEDS-2, un projet qui a été lancé en janvier 2020 et qui vise à s'attaquer aux produits du crime sur Internet et à faciliter la collecte de preuves électroniques en Europe du Sud-Est et

en Turquie. Ce projet fera fond sur les résultats engrangés lors de la mise en œuvre du projet iPROCEEDS et met l'accent sur la fourniture d'un appui ciblé dans les domaines suivants : a) législation relative à l'acquisition de preuves électroniques et à l'accès aux données dans le plein respect des droits et libertés fondamentaux, y compris le respect de la vie privée et la protection des données personnelles ; b) harmonisation avec les normes de protection des données personnelles de l'Union européenne et du Conseil de l'Europe ; c) promotion de politiques et stratégies en matière de cybercriminalité et de cybersécurité ; d) coopération interinstitutions et coopération secteur public-secteur privé aux fins d'enquêtes sur la cybercriminalité et sur les produits du crime sur Internet ; e) systèmes de communication publics sur la fraude en ligne et d'autres crimes ou délits en ligne ; f) formation des magistrats en matière de cybercriminalité, de preuves électroniques, d'enquêtes financières et de mesures de lutte contre le blanchiment d'argent ; g) coopération internationale et partage d'information aux fins d'enquête sur la cybercriminalité et sur les produits du crime sur Internet. Ce projet est appelé à durer quarante-deux mois.

Le Ministère de la sécurité fait office, avec succès, de point de contact pour la mise en œuvre des mesures de confiance de l'OSCE. La communication et la transmission fructueuses d'informations sur la cybersécurité en Bosnie-Herzégovine, la participation aux travaux du Groupe de travail interministériel créé en vertu de la Décision 1039 du Conseil permanent, la participation à sept vérifications des communications et l'organisation d'une formation infrarégionale sur la cybersécurité et la sécurité des TIC sont autant d'exemples d'activités que la Bosnie-Herzégovine a menées au cours de la période à l'examen.

La Bosnie-Herzégovine a en outre pris part au projet régional intitulé « Renforcement des capacités des praticiens de la justice pénale aux fins de la lutte contre la cybercriminalité et la criminalité facilitée par l'environnement numérique ». Le projet a été financé par les Gouvernements de l'Allemagne et des États-Unis d'Amérique et est exécuté par le Département des menaces transnationales de l'OSCE, avec le concours des représentants des pays de la région (Albanie, Bosnie-Herzégovine, Monténégro, Kosovo [1] et Macédoine du Nord) et des missions de l'OSCE sur le terrain. L'objectif premier de ce projet est de former les experts de la lutte contre la cybercriminalité et de la criminalité associée aux technologies numériques. Ce projet a été mis en œuvre entre 2017 et 2019 et a contribué à l'élaboration d'un cadre stratégique global pour la lutte contre la cybercriminalité et les menaces pour la cybersécurité ; il a également permis de renforcer les capacités existantes aux fins de la lutte contre la cybercriminalité et les autres menaces pour la cybersécurité. Le Ministère de la sécurité est responsable de la coordination du projet en Bosnie-Herzégovine.

Le Ministère de la défense entreprend des activités afin d'assurer l'efficacité et la pérennité du système de cybersécurité sous sa juridiction d'ici 2023. Il a notamment adopté une stratégie de cybersécurité pour le secteur de la défense le 4 octobre 2017. Le plan détaillé de mise en œuvre de la stratégie a été adopté quant à lui le 27 décembre 2017. Les objectifs en matière de sécurité concernent avant tout la prévention des atteintes à la sécurité et la réponse à celles-ci, la formation et la certification du personnel de cybersécurité du secteur bosnien de la défense et la sensibilisation des utilisateurs finaux à la sécurité des TIC. Afin d'atteindre ces objectifs, le Ministère de la défense a déjà élaboré ou adopté certains documents de mise en œuvre.

Le Ministère de la défense a en outre lancé les procédures pour la création d'une équipe d'intervention en cas d'atteinte à la sécurité informatique en son sein.

[1] Cette appellation est sans préjudice de la position de la Bosnie-Herzégovine quant au statut du Kosovo.

Dans le cadre du Partenariat pour la paix de l'Organisation du Traité de l'Atlantique Nord, le Ministère de la défense de Bosnie-Herzégovine a l'obligation d'appliquer l'objectif G7300 du partenariat sur la cyberdéfense qui prévoit : a) l'adoption de politiques, procédures et autres documents afin d'intégrer la cyberdéfense aux opérations et aux procédures de planification des opérations et l'application de règlements internationaux dans le cyberespace, de mesures de sécurité pour l'échange des risques et d'évaluations de la menace au sein des organismes nationaux et internationaux compétents en matière de cybersécurité ; b) la création d'une équipe d'intervention en cas d'atteinte à la sécurité informatique ; c) le développement des capacités nécessaires pour assurer la confidentialité, la disponibilité et l'authenticité des informations et des systèmes d'information du Ministère de la défense et des Forces armées de Bosnie-Herzégovine ; d) l'adoption de programmes de qualification et de formation des experts sur le terrain et des utilisateurs finaux ; e) l'adoption de programmes d'enseignement prévoyant des exercices et séminaires sur l'environnement numérique et la participation de représentants du Ministère de la défense et des Forces armées de Bosnie-Herzégovine à ces manifestations.

À l'initiative du Ministère des transports et des communications et avec le concours du Ministère de la sécurité, le Conseil des ministres a adopté, à sa quatre-vingt-quinzième session, le 22 mars 2017, la Politique 2017-2022 sur la gestion de la sécurité de l'information pour les institutions de Bosnie-Herzégovine.

Avec l'appui du Ministère de la sécurité, le Ministère des transports et des communications est en train d'harmoniser, la loi sur la sécurité de l'information et la sécurité des réseaux et systèmes informatiques avec la Directive 2016/1148 de l'Union européenne concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Il élabore également un rapport d'évaluation sur les capacités en matière de cybersécurité de la Bosnie-Herzégovine avec le concours du Global Cyber Security Capacity Center, de l'Université d'Oxford, de la Banque mondiale et du Global Centre for Cyber Security Development, entre autres.

En ce qui concerne ses activités futures, le Ministère des transports et des communications entend soumettre un projet de loi sur l'identification électronique pour les services confidentiels et les transactions électroniques ainsi qu'un projet de stratégie sur le développement de la société de l'information en Bosnie-Herzégovine.

Au niveau des organismes fédéraux de Bosnie-Herzégovine

L'Administration fédérale de police reconnait l'importance de la cybersécurité et a, à ce titre, créé une unité consacrée à la cybercriminalité en 2015. Ladite unité et le Centre d'analyse criminalistique disposent tous deux du personnel, des connaissances et de l'équipement suffisants. L'unité de cybercriminalité compte en son sein 10 experts et le Centre est membre du Réseau européen des instituts de police scientifique. Avec le concours du Fonds des Nations Unies pour l'enfance, d'Emmaüs International et de Save the Children, le Centre prend également une part active, à l'exécution d'un projet sur la prévention de l'exploitation sexuelle des enfants et des atteintes sexuelles commises contre eux sur Internet en Bosnie-Herzégovine. En outre, il a joué un rôle de premier plan dans la mise en œuvre des projets susmentionnés, y compris le projet iPROCEEDS et le projet intitulé « Renforcement des capacités des praticiens de la justice pénale aux fins de la lutte contre la cybercriminalité et la criminalité facilitée par l'environnement numérique ». Il a également joué un rôle central dans l'exécution du projet iPROCEEDS-2.

En 2018, la Fédération de Bosnie-Herzégovine a adopté la Décision portant création du Groupe de travail pour les interventions d'urgence dans le domaine

informatique pour les institutions de la Fédération de Bosnie-Herzégovine, dont les buts et objectifs sont semblables à ceux des deux entités mentionnées précédemment.

Republika Srpska

Le Ministère de l'intérieur de la Republika Srpska indique qu'un certain nombre d'activités ont été entreprises afin d'harmoniser sa législation avec celle de l'Union européenne. À cette fin, il a adopté des orientations de développement pour la période 2017-2021 ainsi qu'un plan d'action pour la mise en œuvre desdites orientations pour la période 2017-2019. Il a également adopté un programme sur le développement des technologies numériques pour la période 2017-2021, qui comprend un objectif relatif à l'amélioration et à l'intégration des systèmes d'information et de communication. La loi sur la police et les affaires internes de la Republika Srpska a ainsi été modifiée de sorte à créer un mécanisme pour l'application du Règlement 910/2014 de l'Union européenne sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et de la Directive 2016/1148 sur la sécurité des réseaux et des systèmes d'information.

À l'initiative du Ministère de l'intérieur de la Republika Srpska, la Loi sur la sécurité des infrastructures critiques (Journal officiel de la Republika Srpska, 58/19) a été adoptée, jetant ainsi les bases de l'application de la Directive 2008/114/CE et de la Directive de l'Union européenne sur la sécurité des réseaux et des systèmes d'information. Les capacités législatives nécessaires ont ainsi été créées et le Ministère a élaboré une définition des infrastructures critiques de sorte à pouvoir réagir à tout incident, y compris dans le domaine informatique.

Le Ministère de l'intérieur de la Republika Srpska a également participé aux projets suivants : projet de 2015 de l'Instrument d'aide de préadhésion, projet intitulé « Renforcement de la qualité et de la sûreté des échanges d'informations entre les services répressifs en Bosnie-Herzégovine », projet intitulé « Renforcement des capacités des praticiens de la justice pénale aux fins de la lutte contre la cybercriminalité et la criminalité facilitée par l'environnement numérique », projets iPROCEEDS et iPROCEEDS-2. Le Ministère développe également les infrastructures nécessaires à un échange sécurisé de données avec d'autres institutions et sujets de droit. Il fournit en outre des services qui s'appuient sur les mécanismes de sécurité prévus par le Règlement de l'Union européenne sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Les documents relatifs à l'introduction de mécanismes contemporains pour la sécurité de l'information sont par ailleurs en cours d'élaboration.

Le Ministère de l'intérieur de la Republika Srpska dispose également d'une unité consacrée à la lutte contre la criminalité liée aux technologies de pointe et, à l'instar des autres services répressifs de Bosnie-Herzégovine, travaille de concert avec l'Organisation internationale de police criminelle, l'Agence de l'Union européenne pour la coopération des services répressifs, l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale, l'Office des Nations Unies contre la drogue et le crime, l'OSCE, l'Agence de l'Union européenne pour la formation des services répressifs, l'ambassade des États-Unis d'Amérique, l'International Criminal Investigative Training Assistance Program, l'Association internationale de police, le Fonds des Nations Unies pour l'enfance et avec bien d'autres ambassades et organisations internationales. Parmi les domaines de coopération figurent notamment l'éducation, la formation, ou encore l'échange de connaissances et de données.

En ce qui concerne les autres entités responsables du maintien de la cybersécurité en Bosnie-Herzégovine, la Republika Srpska a adopté, en 2011, la loi

sur la sécurité de l'information (Journal officiel de Republika Srpska, 70/11), qui énonce les règles fondamentales applicables à la sécurité de l'information. En vertu de cette loi, une Équipe d'intervention d'urgence dans le domaine informatique a été créée au sein de l'ex-Agence de la société de l'information de Republika Srpska (qui est désormais le Ministère du développement scientifique et technologique, de l'enseignement supérieur et de la société de l'information), entité responsable de la sécurité de l'information. Elle a pour mandat de coordonner la prévention des atteintes à la sécurité informatique et de protéger les infrastructures numériques des organismes publics et des personnes morales et physiques. Ces deux dernières années, l'Équipe a également mis sur pied le Centre des opérations de sécurité du Gouvernement de la Republika Srpska, dont le but est de protéger les infrastructures pertinentes du point de vue de la sécurité de l'information. Les membres du Centre ont été formés et travaillent aujourd'hui dans le cadre de trois équipes qui se relaient en continu. Le Centre œuvre d'arrache-pied pour être accrédité par les organisations internationales pertinentes ou en devenir membre.

Canada

[Original : anglais, français]
[7 mai 2020]

Par rapport à la cybersécurité, le Canada :

- est déterminé à promouvoir la stabilité internationale, ainsi qu'un cyberespace libre, ouvert et sécuritaire ;
- estime que le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États et renforce la stabilité dans le cyberespace ;
- invite les États à respecter les normes acceptées pour le comportement étatique dans le cyberespace, y compris les normes énoncées dans le rapport du GEG de l'ONU de 2015, qui a été approuvé par l'Assemblée générale des Nations Unies (AGNU) ;
- croit que les mesures de renforcement de la confiance (MRC) sont une méthode éprouvée pour renforcer la stabilité dans le cyberespace.

Au niveau national, le Canada est actif de plusieurs façons :

- En juin 2018, le Gouvernement, sous la direction de Sécurité publique Canada, a publié sa Stratégie nationale de cybersécurité (SNCS). La Stratégie vise à consolider les partenariats en vue de protéger les cybersystèmes essentiels à l'intérieur et à l'extérieur du Gouvernement fédéral et à protéger les Canadiens et les entreprises canadiennes qui utilisent l'Internet. Elle vise également à améliorer la détection des cybermenaces en évolution constante et la capacité d'y répondre. La SNCS est organisée en fonction de trois objectifs de haut niveau : 1) Des systèmes canadiens sécurisés et résilients ; 2) Un écosystème du cyberespace novateur et adaptable ; 3) Leadership, gouvernance et collaboration. Le Gouvernement du Canada met en œuvre les objectifs de la SNCS dans le cadre du Plan d'action national en matière de cybersécurité de 2019, qui énonce des initiatives particulières sur cinq ans.
- Dans le cadre de la mise en œuvre de sa SNCS, le Canada a créé le Centre canadien pour la cybersécurité, qui regroupe les unités opérationnelles de cybersécurité du Gouvernement du Canada en une seule organisation publique. À titre d'Équipe d'intervention en cas d'urgence informatique (EIUI) du Canada, le Centre pour la cybersécurité est une source unifiée de conseils, de

directives, de services et de soutien spécialisés pour le Gouvernement, les propriétaires et les exploitants d'infrastructures essentielles, le secteur privé et le public canadien.

- La SNCS comprend aussi le financement de la nouvelle Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC). Bien que gérée par la Gendarmerie royale du Canada (GRC), l'UNCLC servira toutes les forces de police canadiennes et collaborera avec les partenaires des secteurs public et privé. L'UNCLC, qui vise à être pleinement opérationnelle d'ici 2023, coordonnera les enquêtes sur la cybercriminalité touchant plusieurs champs de compétence au Canada et à l'étranger et résoudra les conflits associés.
- La GRC a aussi reçu du financement additionnel en 2018 pour augmenter ses capacités opérationnelles en matière de renseignement et d'enquête. Ce financement a aussi servi à renforcer l'expertise technique spécialisée de la GRC pour appuyer sa capacité de contrer la cybercriminalité domestique et internationale.

Sur le plan international, le Canada est actif de plusieurs façons :

- Le Canada participe, avec la communauté internationale, les États aux vues similaires et des pays alliés à de nombreux forums pour renforcer l'environnement international de cybersécurité. Le Canada continue notamment à promouvoir le développement du droit international et le respect des normes convenues de comportement étatique dans le cyberespace, y compris les normes décrites dans le rapport du GEG de 2015 et approuvées par l'AGNU. Le Canada participe également activement au Groupe de travail à composition non limitée (GTCNL) de l'ONU et se prononce, au besoin, sur les discussions en cours du GEG. Le Canada espère que le GTCNL favorisera la mise en œuvre des normes convenues et abordera entre autres les aspects de la cybersécurité liés au genre.
- Dans les forums multilatéraux de l'ONU, le Canada travaille en vue de faire progresser les normes et standards en matière de droits humains. Le Canada encourage aussi les États à respecter leurs obligations à cet égard. Ceci inclut répondre à la violence contre les femmes et les filles facilitée par les TIC, ainsi qu'assurer leur sécurité et intégrité personnelle dans les contextes en ligne et hors ligne. Le Canada tente de faire des progrès sur ces objectifs de diverses façons, incluant en chaperonnant une résolution au Conseil des droits de l'homme qui vise à éliminer la violence contre les filles et les femmes dans les contextes numériques.
- Guidé par sa politique de défense *Protection, sécurité et engagement* de 2017, le Canada prend des mesures pour dissuader les cyberactivités malveillantes et y répondre, notamment en mettant à profit ses cybercapacités pour soutenir les opérations militaires. La cybercapacité active des Forces armées canadiennes est assujettie à la même rigueur que ses autres capacités militaires, y compris au droit national et international applicable, ainsi qu'aux règles d'engagement.
- Au Sommet du G7 à Charlevoix en juin 2018, les dirigeants ont annoncé la création du Mécanisme de réponse rapide (MRR). Le MRR a pour mandat de coordonner les efforts au sein du G7 afin de cerner les menaces diverses et changeantes qui pèsent sur nos démocraties, dont la désinformation, et d'y réagir, notamment en échangeant de l'information et des analyses, ainsi qu'en identifiant les possibilités de réponse coordonnée. Le MRR vise à contrer un large éventail de menaces à la démocratie, dans l'intérêt des membres du G7 et de la communauté internationale en général.

Quelques autres efforts internationaux en cours :

- Depuis 2015, le Canada a injecté plus de 4 millions de dollars pour le soutien de projets de renforcement des capacités en matière de cybersécurité. Le Canada a aussi financé la participation de femmes diplomates des Amériques au GTCNL de l'ONU, dans le contexte du Programme de bourses pour les femmes dans le domaine de la sécurité internationale et du cyberespace. Ce programme vise à promouvoir la participation accrue des femmes aux discussions onusiennes sur les questions de cyber sécurité.
- Le Canada appuie les efforts de l'OTAN visant à renforcer les capacités de cyberdéfense de l'Alliance et de ses divers alliés.
- Le Canada travaille à la mise en œuvre des MRC dans diverses tribunes, dont l'OSCE, l'OEA et le Forum régional de l'ANASE.
- Le Canada est un membre actif de la Coalition pour la liberté en ligne, une organisation internationale multilatérale qui fait la promotion des droits humains en ligne. Le Canada préside un groupe de travail multipartite sur l'intelligence artificielle et les droits humains.

Le Canada demeure déterminé à faire progresser les efforts mondiaux visant à assurer la sécurité et la stabilité dans le cyberespace, au profit de tous.

Colombie

[Original : espagnol]
[29 mai 2020]

En application de la résolution 74/28 de l'Assemblée générale de l'ONU, intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », la Colombie a le plaisir de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, ses vues et observations sur les questions suivantes :

- les efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine ;
- la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

Introduction

La Colombie, qui est favorable à un environnement numérique libre, ouvert, sûr et propre à garantir la neutralité de l'Internet, estime de manière générale qu'il importe de continuer de mettre l'accent sur le renforcement des capacités et la coopération, ancrées dans le droit international et les normes et conventions existantes, et sur la mise en œuvre de mesures de confiance dans le cyberespace.

Dans le domaine de la sécurité numérique et pour ce qui est du cyberespace, la Colombie a fait d'importants efforts et mise sur une concertation interinstitutionnelle au plus haut niveau propre à garantir un cyberespace plus sûr.

Sur la base de la politique publique de sécurité numérique adoptée en 2016, le pays s'est doté d'un Comité de sécurité numérique réunissant les entités compétentes en la matière et chargé de coordonner la riposte en cas d'éventuelles crises nationales de cybersécurité. Ce comité est dirigé par un coordinateur national, fonction actuellement occupée par le conseiller présidentiel aux affaires économiques et à la

transformation numérique. Le secrétariat technique est assuré par le Ministère des technologies numériques.

La structure institutionnelle en place vise à organiser la confluence entre l'étude et la mise à jour des politiques et réglementations concernant la sécurité numérique, l'examen des priorités internationales et les mesures de défense et de sécurité nationale dans l'environnement numérique, de façon à amortir ou contrer les cyberattaques, à protéger les infrastructures nationales critiques et renforcer les capacités humaines, techniques, technologiques et physiques, les entités concernées étant les suivantes :

- **Groupe colombien d'intervention en cas d'atteinte à la sécurité informatique**. Organe du Ministère de la défense responsable de coordonner les actions nécessaires pour protéger les infrastructures critiques de l'État colombien en cas d'événements mettant en jeu la cybersécurité et menaçant ou compromettant la sécurité et la défense nationales. Le Groupe est compétent en cas d'incidents informatiques.
- **Commandement cybernétique conjoint des forces armées**. Organe faîtier chargé de diriger, planifier, coordonner, intégrer, exécuter et synchroniser les opérations cybernétiques conjointes. Responsable de la cyberdéfense et des opérations cybernétiques militaires de niveau stratégique, il est garant de la sécurité et de la défense de la nation dans le cyberespace, y compris la coordination des infrastructures critiques.
- **Centre cybernétique de la police**. Unité de la direction des enquêtes criminelles et des rapports avec Interpol de la Police nationale, elle est chargée de développer des stratégies, des programmes et des projets relatifs à la sécurité numérique, la cybersécurité et la protection des informations et des données circulant dans le cyberespace relatives aux habitants du territoire national, les enquêtes criminelles étant le mode d'action privilégié.
- **Équipes d'intervention en cas d'atteinte à la sécurité informatique**. Il existe en Colombie des équipes d'intervention respectivement consacrées aux autorités publiques, aux institutions financières, aux enjeux sectoriels ou à des groupes privés. Au niveau régional, dans le cadre de l'Organisation des États américains (OEA), la Colombie fait partie du réseau hémisphérique d'équipes d'intervention en cas d'atteinte à la sécurité informatique des Amériques, réseau qui a pour vocation d'améliorer la communication des alertes dans la région.

La Colombie est convaincue de la nécessité de renforcer la coordination et la coopération entre États en ce qui concerne l'étude des menaces et des mesures conjointes qui pourraient être envisagées pour y faire face. L'importance de la coopération internationale ne saurait être surestimée, non seulement du point de vue du transfert de connaissances, de technique et de meilleures pratiques, mais aussi de la concertation des interventions.

Pour les pays moins développés sur le plan technologique, il est primordial de parvenir à des conciliations et accords à même d'empêcher que le cyberespace ne devienne le théâtre de conflits dont nous pourrions subir les conséquences, soit parce que nous serions les cibles d'opérations cybernétiques, soit parce que, faute d'avoir les capacités suffisantes pour contrer celles-ci, nous nous en rendrions complices.

Dans ces pays, en effet, toute atteinte aux infrastructures critiques peut avoir de graves répercussions : alors même que tout ce qui a trait à l'informatique ou à l'automation des procédés industriels dépend d'Internet et des technologies connexes, la conscience des risques et menaces et les ressources qu'il faudrait consacrer à la sécurisation numérique des entreprises exploitant ces infrastructures font défaut.

L'insuffisance des capacités est donc elle-même un facteur de risque, ce qui nous met en demeure d'établir des mécanismes de coopération internationale consacrés à l'étude des risques et au renforcement des capacités.

Le défaut de catégorisation des risques et l'insuffisance des mesures de prévention et de protection des activités critiques sont autant de dangers pour les États moins avancés en matière de sécurité numérique. Ces États souffrent par ailleurs d'un manque de dispositifs de gouvernance sur la sécurité numérique, risque qui entrave en outre la concertation au niveau interinstitutionnel et international.

Ces nouvelles menaces – et celles qui pourraient surgir à l'avenir étant donné le rythme vertigineux auquel se développent les technologies – mais aussi la question du comportement responsable des États dans le cyberespace et celle de la sécurité des technologies numériques doivent être abordées dans une perspective transnationale sans laquelle aucune solution n'est permise. L'heure est donc à la concertation des efforts, pour ce qui est non seulement de la bonne communication des informations – ce qui comprend l'échange responsable des informations sur les vulnérabilités – mais aussi de la riposte efficace à d'éventuelles menaces.

Répétons-le, la Colombie est pleinement disposée à continuer d'œuvrer à la coordination et au renforcement de la coopération s'agissant de l'étude des menaces avérées ou en puissance et des mesures conjointes qui pourraient être envisagées pour y faire face.

Normes, règles et principes internationaux de comportement responsable des États

La Colombie souscrit pleinement aux idées, considérations, interprétations et recommandations consignées dans les rapports du Groupe d'experts gouvernementaux, en particulier le rapport de 2015, qui s'inspirait des travaux précédents et dont l'Assemblée générale a repris les conclusions cette même année à titre de guide à l'usage des États Membres sur l'utilisation de technologies numériques.

L'urgence est à présent de les faire connaître et appliquer. Un instrument juridiquement contraignant n'a pour l'instant pas lieu d'être.

Il importe en outre que le texte bénéficie d'une coopération internationale venant donner aux États de meilleurs moyens de l'appliquer.

Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, la Colombie se tient prête à coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité de l'utilisation des technologies numériques, et à prévenir les pratiques informatiques jugées nocives ou susceptibles de compromettre la paix et la sécurité internationales.

Ainsi, le 23 septembre 2019, le pays a appuyé la déclaration que les États-Unis avaient proposée sur le comportement responsable des États dans le cyberespace, dans laquelle plusieurs pays se sont conjointement engagés à garantir la responsabilité et la stabilité dans le cyberespace et, pour ce faire, à s'efforcer ensemble de contrer et de dissuader plus efficacement les activités cybernétiques malveillantes aux effets perturbateurs, destructeurs ou déstabilisants. Le comportement responsable dans le cyberespace suppose que l'État agisse en fonction du droit international, qu'il en respecte en temps de paix les normes non contraignantes et qu'il prenne des mesures de confiance concrètes.

La Colombie souscrit aussi à l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, initiative du Gouvernement français annoncée le 12 novembre 2018 et visant à l'élaboration de principes communs à même de sécuriser le

cyberespace, appel auquel plusieurs pays, entreprises privées et organisations de la société civile ont réservé un accueil favorable.

Elle souscrit également à l'Appel de Christchurch pour agir contre le terrorisme et l'extrémisme violent en ligne, initiative des Gouvernements français et néozélandais lancée en mai 2019.

Au plan interne, elle s'est dotée de politiques publiques consignées dans des documents du Conseil national de la politique économique et sociale. En 2011, elle a formellement élevé la cybersécurité et la cyberdéfense au rang d'éléments fondamentaux de la défense nationale dans le document 3701 du Conseil, qui contient les grandes orientations politiques en la matière et qui visait généralement à doter l'État de meilleurs moyens pour parer aux menaces contre la sécurité et la défense touchant au domaine cybernétique (cybersécurité et cyberdéfense) et, pour ce faire, à instaurer les conditions voulues pour assurer la protection du cyberespace. Trois grands axes y sont envisagés : a) création des structures institutionnelles touchant au cybernétique et définition des grandes orientations concernant le renforcement des moyens publics de lutte contre les menaces affectant le cyberespace ; b) instauration des dispositifs d'amélioration des capacités concernant la sécurité informatique et multiplication des axes de recherche ; et c) renforcement de la législation en matière de cybersécurité.

Par le document 3854 du Conseil, définissant la politique nationale en matière de sécurité numérique et daté de 2016, la Colombie a cherché à renforcer quatre grands volets : a) cadre institutionnel ; b) capacités des parties prenantes à reconnaître, gérer, traiter et atténuer les risques attenants à la sécurité numérique des activités socioéconomiques dans le cyberespace ; c) progrès de la responsabilité partagé ; d) prise en compte de la gestion des risques dans les activités des parties prenantes en milieu numérique.

Une politique publique de confiance et sécurité numérique, en cours d'élaboration depuis 2019, vise entre autres à évaluer et mettre à jour, de manière à les développer, les dispositifs de gouvernance encadrant la sécurité numérique. L'une des propositions concerne la création d'un système national de gestion des incidents cybernétiques, qui aurait pour vocation : i) de structurer les efforts institutionnels visant à la bonne gestion des incidents cybernétiques ; ii) de servir de source officielle de statistiques sur les incidents cybernétiques constatés dans le pays ; iii) de normaliser les dispositifs de communication périodique d'incidents et de vulnérabilités cybernétiques, l'objectif étant de les reconnaître, de les évaluer et de les communiquer aux intéressés ; iv) de servir au Gouvernement national de source d'inspiration pour la prise de décisions. Des progrès sont attendus quant à l'aspect technique du système, et les informations qui y sont consignées pourront être consultées en temps réel par les organismes de sécurité de l'État.

En outre, la transformation stratégique, la coopération internationale en matière de sécurité et l'innovation, la science et la technologie au service du renforcement des capacités du secteur de la défense figurent parmi les grands axes de la politique de défense et de sécurité colombienne.

La cybersécurité et la cyberdéfense sont également abordées sous l'angle de la diplomatie, et plus concrètement de la sécurité coopérative et de l'internationalisation, certaines alliances stratégiques étant passées à cette fin – le pays est par exemple partenaire mondial de l'Organisation du Traité de l'Atlantique Nord pour ce qui est de l'échange des connaissances et a passé un programme individuel de partenariat et de coopération, l'objectif étant de renforcer les capacités des forces armées et leur coordination face aux menaces et pour la défense du cyberespace.

La Colombie a également adopté des lignes directrices inspirées des bonnes pratiques et des normes internationales concernant la création et le fonctionnement des équipes d'intervention en cas d'atteinte à la sécurité informatique. Ces lignes directrices, qui concernent les secteurs privé, public et mixte, portent sur la gestion opérationnelle des atteintes à la cybersécurité affectant les intérêts nationaux et visent à favoriser la coopération, la collaboration et l'assistance en matière de sécurité numérique, de cybersécurité et de cyberdéfense avec les membres des équipes d'intervention des Amériques et d'Europe, aux fins de l'échange d'informations et de bonnes pratiques.

Le Commandement cybernétique conjoint est membre du Forum ibéroaméricain de cyberdéfense, qui vise à améliorer la coopération, à partager les enseignements tirés de l'expérience, à renforcer les capacités de gestion des risques et de lutte contre les menaces transnationales dans le cyberespace et à participer aux exercices nationaux et internationaux.

Le Centre cybernétique de la police a mis en place un centre de formation à la cybersécurité en Colombie chargé de procéder à des analyses, à des alertes de prévention et à certaines activités liées à la gestion des incidents de cybersécurité et de diligenter des enquêtes en cas de cybercriminalité.

La Commission de réglementation des communications est quant à elle chargée des fonctions suivantes : i) créer des mécanismes favorisant la coopération en matière de sécurité numérique entre les prestataires de services de télécommunications et le Groupe colombien d'intervention en cas d'atteinte à la sécurité informatique ; ii) centraliser à l'échelle du secteur les renseignements sur les atteintes à la sécurité informatique des exploitants ; iii) fournir au Groupe d'intervention les informations voulues pour gérer les incidents et y sensibiliser les intéressés, dans l'intérêt des diverses parties prenantes.

Le texte de référence à cet effet est la résolution 5569 de la Commission, en date de 2018, qui fait obligation aux opérateurs des réseaux et des services de télécommunications de mettre en place un système de gestion et de sécurité de l'informatique et d'adopter des procédures propres à garantir l'intégrité, la confidentialité et la disponibilité des données.

Signalons que les textes réglementaires concernant la sécurité numérique prennent en compte les recommandations formulées par l'Organisation de coopération et de développement économiques dans l'ouvrage intitulé « La gestion du risque de sécurité numérique pour la prospérité économique et sociale ».

Ces recommandations posent comme première étape de la gestion des risques pour la sécurité numérique la définition des objectifs économiques et sociaux liés à la sécurité et l'élaboration d'activités spécifiques, de façon à ce que, lors de la phase de gestion des risques, le niveau de risque de l'activité en question puisse être déterminé, compte tenu de son incidence possible sur les objectifs sociaux et économiques.

À la phase de traitement du risque, il convient de déterminer en quoi la stratégie doit être modifiée pour augmenter les chances de succès de l'activité tout en préservant les objectifs définis ; c'est de cette évaluation que dépend la décision de prendre, d'atténuer, de transférer ou d'éviter le risque. Si l'atténuation s'impose, on choisira les mesures de sécurité à prendre, y compris des mesures novatrices, ou des mesures de préparation au traitement.

En cas de problème, la Colombie examine donc toutes les informations pertinentes, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans le domaine du numérique et la nature et l'ampleur des conséquences.

Plus concrètement, en ce qui concerne la caractérisation des incidents et leur communication obligatoire aux autorités compétentes, la réglementation de la Commission incorpore les grandes orientations et bonnes pratiques consignées dans les normes ISO/IEC 27000 (en particulier les catégories proposées au titre de la norme ISO 27035-1) pour ce qui est des incidents touchant à la sécurité de l'information. La réglementation prévoit en effet que, lorsqu'un tel incident survient, les opérateurs de réseaux ou de services de communication sont tenus de le signaler par voie électronique au Groupe d'intervention en cas de cyberurgence après avoir contenu, éliminé ou arrangé le problème.

La recommandation faite aux États de ne pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques est reprise en tête du document qui nous occupe ; le Comité de sécurité numérique – qui réunit les autres instances publiques compétentes, à savoir le Groupe d'intervention colombien en cas d'atteinte à la sécurité informatique, le Commandement cybernétique conjoint des forces armées, le Centre cybernétique de la police et l'équipe d'intervention d'urgence des autorités publiques – est l'organe chargé de procéder dans le pays aux activités de prévention et d'intervention face aux incidents cybernétiques, de quelque catégorie ou type qu'ils relèvent, sur tout le territoire.

Sur le plan international, la Colombie s'emploie à coopérer par le biais de l'échange d'informations, de l'entraide et des poursuites pénales en cas d'utilisation terroriste ou criminelle des technologies numériques. Elle met également en œuvre d'autres mesures de coopération pour faire face à ces menaces.

À cet égard, le nouveau document du Conseil national de politique économique et sociale sur la confiance et la sécurité numérique, en cours d'élaboration, prévoit le développement et la mise en service d'un système d'échange d'informations numériques, l'objectif étant de faciliter la diffusion d'indicateurs relatifs aux engagements pris par les acteurs du milieu numérique aux niveaux national et international. Ce système sera relié au registre central unique répertoriant les atteintes à la sécurité numérique.

Le Bureau du Procureur général coopère selon les modalités prévues dans les conventions bilatérales et multilatérales. Toutefois, il est nécessaire de créer un canal sécurisé ou un service Web permettant de demander et de recevoir directement des informations de la part des fournisseurs d'accès à l'Internet, pour la plupart privés, l'objectif étant que les demandes puissent être envoyées, reçues, échangées et étudiées de façon à raccourcir les délais de réponse aux demandes d'entraide judiciaire.

Les mécanismes actuels de traitement des demandes sont trop lents, ce qui pose des problèmes de procédure. Les réponses arrivent en effet tellement tard dans l'enquête qu'elles ne peuvent plus être prises en compte dans la procédure pénale.

Ainsi, la Direction nationale du renseignement s'est mise en contact avec ses homologues dans certains pays afin de procéder à un échange d'informations opérationnelles en temps voulu et afin de demander des compléments d'information pour des cas spécifiques nécessitant des recherches ou une confirmation.

Cette coordination sert à réunir des informations supplémentaires sur les cas où les tendances recensées dans le cyberespace, pour lesquelles la corrélation d'événements ou l'historique des activités sont nécessaires à la mise en place de processus de surveillance des acteurs hostiles, actifs dans le cyberespace.

La Cour constitutionnelle colombienne s'est prononcée à plusieurs reprises sur la recommandation selon laquelle les États, lorsqu'ils veillent à une utilisation sûre des technologies numériques, respectent les résolutions 20/8 et 26/13 du Conseil des

droits de l'homme, sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 sur le droit à la vie privée à l'ère du numérique, afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression,.

En Colombie, conformément à l'arrêt d'unification SU-420 de 2019, le droit à la liberté d'expression s'applique sur Internet comme dans les autres médias ; autrement dit, les réseaux sociaux ne doivent pas être un moyen de véhiculer des propos diffamatoires et, bien qu'il ne soit pas possible de subordonner la publication de contenus à un permis ou à une autorisation préalable, la primauté relative de la liberté d'expression ne signifie pas que celle-ci soit sans limites, de sorte que l'exercice d'un tel droit emporte la responsabilité à l'égard d'autrui.

La Commission de réglementation des communications a publié la résolution 5111 de 2017 portant entre autres création du régime de protection des droits des utilisateurs de services de communications et modification du chapitre 1 du titre II de la résolution CRC 5050 de 2016. En vertu de ce régime, les fournisseurs de réseaux et de services de télécommunications sont tenus d'utiliser des outils technologiques appropriés pour prévenir la fraude sur leurs réseaux et de contrôler régulièrement que ceux-ci sont efficaces. Cependant, si un utilisateur dépose une demande, une plainte, une réclamation ou un recours qui peut être lié à une fraude présumée, le fournisseur est tenu de mener l'enquête.

Afin de déterminer quels sont les éléments qui, sur le plan de la loi ou du règlement, sont nécessaires à la promotion de la sécurité numérique et au renforcement des capacités, la nouvelle politique sur la confiance et la sécurité numérique, qui est en cours d'élaboration, prévoit un diagnostic visant à recenser les normes qui pourraient faire l'objet d'ajustements dans des domaines tels que : a) la sécurité des technologies numériques ; b) la protection et la défense du droit à la vie privée et du droit à la liberté d'expression et des autres droits de la personne en ligne ; c) le signalement responsable des failles ; d) la protection des données ; e) la protection du consommateur ; f) la gestion des risques et des incidents ; g) les centres d'intervention en cas d'incident, ou tout autre centre jugé nécessaire ; h) la constitution d'équipes sectorielles d'intervention en cas d'atteinte à la sécurité informatique. Ce diagnostic sera effectué en prenant en compte les nombreuses parties concernées. Il devra permettre de déterminer comment apporter les ajustements nécessaires au cadre législatif et réglementaire en vigueur.

En ce qui concerne les recommandations selon lesquelles les États prennent les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies numériques, la Colombie s'emploie, outre ce qui précède, à élaborer, en coordination avec les différentes parties prenantes, le plan de sécurité et de défense des infrastructures numériques critiques, qui contient des directives générales destinées aux organisations du secteur. Ce document est une première étape visant à renforcer et à harmoniser les efforts de protection des infrastructures désignées comme critiques.

Sur le plan international, comme indiqué ci-dessus, la Colombie coopère et donne suite aux demandes d'aide que lui adressent d'autres États, l'objectif étant de limiter les conséquences des activités numériques malveillantes. À cet égard, elle a adhéré à la Convention sur la cybercriminalité le 16 mars 2020. De même, elle a adopté des mesures visant à garantir l'intégrité de la chaîne d'approvisionnement, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits numériques.

En ce qui concerne le signalement responsable des failles numériques et la communication des informations sur les moyens de les corriger afin de limiter voire

d'éliminer les menaces qu'elles pourraient constituer pour les systèmes et les infrastructures qui utilisent les technologies numériques ou en dépendent, la nouvelle politique sur la confiance et la sécurité numérique, qui est en cours d'élaboration, envisage la mise en place d'une procédure de promotion et de signalement responsable des failles des systèmes d'information et des infrastructures technologiques des entités publiques, qui pourront ainsi les corriger.

Dans la politique nationale de sécurité numérique, établie en 2016 en vertu du document 3854 du Conseil national de politique économique et sociale, le Gouvernement colombien a formulé de grandes orientations pour la mise sur pied d'équipes d'intervention cybernétique d'urgence ou d'équipes d'intervention en cas d'atteinte à la sécurité informatique.

Mesures de confiance volontaires

Pour la Colombie, il est capital de continuer à œuvrer à l'élaboration et à l'adoption de mesures de confiance et de sécurité dans le cyberespace. Au niveau régional, des travaux ont été réalisés à cette fin par l'intermédiaire de l'OEA.

En avril 2017, sur l'initiative du Canada, des États-Unis, du Chili, du Mexique et de la Colombie, une résolution a été adoptée portant création d'un groupe de travail sur les mesures de coopération et de confiance dans le cyberespace, qui relève du Comité interaméricain contre le terrorisme de l'OEA. En février 2018, la Colombie a été élue à la présidence de ce groupe de travail, puis elle a cédé sa place au Chili lors de la deuxième réunion du groupe, tenue au Chili en avril 2019.

Les mesures de confiance en matière de cybersécurité adoptées par l'OEA sont les suivantes :

1. Fournir des informations sur les politiques nationales en matière de cybersécurité telles que stratégies nationales, livres blancs, cadres juridiques et autres textes jugés pertinents par tel ou tel État ;

2. Désigner un point de contact national au niveau politique pour discuter des conséquences des menaces numériques dans l'hémisphère ;

3. Désigner au Ministère des affaires étrangères, si ce n'est pas déjà fait, des points de contact devant faciliter, à l'échelle internationale, la coopération et les dialogues sur la cybersécurité et le cyberespace ;

4. Développer et renforcer les capacités par le biais d'activités telles que séminaires, conférences et ateliers sur la diplomatie numérique, organisées au profit des fonctionnaires publics et privés ;

5. Encourager la prise en compte des questions de cybersécurité et du cyberespace dans les cours de formation de base et de formation des diplomates et des fonctionnaires des ministères des affaires étrangères et autres services de l'État ;

6. Promouvoir la coopération et la mise en commun des meilleures pratiques en matière de diplomatie numérique, de cybersécurité et de cyberespace par la création de groupes de travail et d'autres mécanismes de dialogue et grâce à la signature d'accords entre États.

Il convient de souligner que des mesures de confiance relatives à la diplomatie numérique en particulier pourraient être un atout ; des travaux en ce sens sont en cours, sous l'égide de l'OEA.

Grâce à la diplomatie numérique, des solutions aux défis du cyberespace peuvent être trouvées. Il faut pour cela non seulement renforcer la participation active des États aux débats internationaux sur les questions de cybersécurité, et donc former

les diplomates à ces questions, mais aussi inviter des experts à jouer un rôle actif dans les instances multilatérales.

Par ailleurs, il convient d'engager des dialogues institutionnels réguliers avec un grand nombre de parties prenantes et d'étendre et de soutenir les pratiques de coopération entre les équipes d'intervention en cas d'urgence informatique et les équipes d'intervention en cas d'atteinte à la sécurité informatique.

S'agissant de la proposition visant à établir une liste complète de points de contact, il est suggéré, à des fins pratiques, de prévoir des catégories différentes, par exemple un point de contact politique ou diplomatique et des points de contact techniques (police, procureurs, équipes d'intervention informatique d'urgence, etc.)

Pour ce qui est de l'information, il faudra déterminer qui en est responsable et s'assurer qu'elle soit toujours mise à jour. Il convient d'envisager un protocole clair et ouvert de gestion de l'information, et notamment des bases de données.

En ce qui concerne plus particulièrement les points de contact nationaux aux niveaux technique et politique pour les atteintes numériques graves, le Ministère des technologies numériques a désigné des responsables de chaque question relative à la sécurité numérique. Ces données peuvent être communiquées aux instances qui les nécessitent.

Par ailleurs, le Ministère des technologies numériques dispose d'un annuaire contenant les coordonnées des directeurs chargés des technologies numériques et des directeurs chargés de la sécurité informatique des entités publiques, ainsi que des nombreuses parties prenantes, avec lesquels des espaces de discussion sur les grandes orientations en matière de sécurité numérique ont été ouverts et des actions coordonnées ont été menées pour chacune des phases de gestion des incidents par les équipes sectorielles d'intervention en cas d'atteinte à la sécurité informatique des services de l'État.

En ce qui concerne la mise en place de mécanismes et de processus de consultation bilatérale, régionale, sous-régionale et multilatérale et des services d'appui y afférents dans le but d'améliorer la confiance entre les États et de réduire le risque de malentendus, d'escalade et de conflit découlant d'incidents informatiques, la Colombie participe activement aux travaux de différentes instances internationales, comme cela a déjà été indiqué.

La Colombie participe notamment aux débats organisés à l'ONU (à New York, Vienne et Genève), ainsi qu'aux mécanismes et manifestations régionaux, principalement dans le cadre de l'OEA.

Dans le cadre du groupe du Plan d'action dans le domaine du numérique de l'Alliance du Pacifique, avec le soutien du réseau de l'OEA réunissant les équipes d'intervention en cas d'atteinte à la sécurité informatique des Amériques, la Colombie participe au projet d'échange d'informations sur les menaces numériques établi entre les États membres de l'Alliance du Pacifique. Ainsi, la plateforme technologique d'échange d'informations entre les équipes d'intervention en cas d'atteinte à la sécurité du cyberspace des pays membres est devenue opérationnelle le 23 janvier 2020. La plateforme nationale de la Colombie est gérée par le Groupe colombien d'intervention cybernétique d'urgence.

Au niveau bilatéral, la Colombie a conclu un mémorandum d'accord avec le Chili sur le cyberespace, la cybersécurité, la cyberdéfense, la cybercriminalité et le cyberrenseignement , signé par les ministres des affaires étrangères le 21 mars 2019. Les parties prenantes colombiennes sont le Conseil présidentiel pour les affaires économiques et la transformation numérique, le Ministère des technologies numériques, le Ministère de la défense, le Centre de formation en cybersécurité de la

police, la Direction nationale du renseignement, le Bureau du Procureur, le Ministère de la justice et le Ministère des affaires étrangères.

Les experts gouvernementaux de la Colombie et du Pérou se sont réunis virtuellement le 15 avril 2020 pour mettre en commun leurs expériences en matière de sécurité numérique. Ils ont échangé des informations sur les politiques et stratégies nationales et ils ont établi un canal de communication pour décider des mesures d'appui à prendre en cas d'atteinte à la sécurité numérique.

En outre, la Colombie est membre des conseils d'innovation dans le domaine de la cybersécurité, une initiative de l'OEA et de Cisco permettant aux principaux dirigeants d'entreprises publiques et privées et à des membres de la société civile et du monde universitaire d'interagir dans le but de promouvoir l'innovation, de sensibiliser les citoyens et de diffuser les meilleures pratiques en matière de cybersécurité dans la région. Ces conseils constituent un maillon important dans la mise en œuvre des mesures de confiance dans le cyberespace et peuvent contribuer à l'application d'une politique de sécurité numérique plus efficace aux niveaux national et international.

Il convient de signaler que les demandes internationales dans le domaine du numérique passent généralement par l'organe chargé de la prévention du crime du Ministère des affaires étrangères.

S'agissant de la promotion de la coopération et plus précisément de la mise en place de centres de coordination permettant d'échanger des informations relatives à l'utilisation malveillante des technologies numériques et de contribuer aux enquêtes, le travail effectué par les différentes autorités et services de l'État en vue d'élaborer un protocole national de gestion des incidents mérite d'être mis en exergue. Ce protocole a pour but d'organiser une coordination rapide pour faire face aux atteintes informatiques susceptibles de menacer l'ordre économique et social ou la sécurité nationale. Il est important d'appliquer ce protocole car il permet de détecter l'atteinte, d'effectuer une étude de cas, d'analyser la menace et de définir les mesures d'endiguement ou de correction.

Le Bureau du Procureur général compte trois groupes chargés des questions relatives à la cybercriminalité, qui apportent leur expertise et leur aide dans le cadre d'enquêtes diligentées suite à des demandes d'entraide judiciaire pour utilisation malveillante des technologies numériques.

Ces groupes sont : a) le Bureau du Procureur adjoint chargé de la lutte contre la criminalité organisée ; b) le Bureau du Procureur adjoint chargé de la sécurité citoyenne ; c) la Direction de la cellule technique chargée des enquêtes. Au sein du Bureau du Procureur, ces groupes d'experts encouragent la diffusion des nouvelles tendances et des bonnes pratiques en matière de lutte contre la cybercriminalité et de preuves numériques, en plus de collaborer aux enquêtes.

La Direction des affaires internationales du Bureau du Procureur s'appuie quant à elle sur les différents procureurs détachés et sur les trois groupes d'experts pour mener les enquêtes liées à la cybercriminalité.

Il convient de souligner l'appui apporté par le Ministère américain de la justice, qui a organisé des formations sur les questions liées aux demandes d'entraide judiciaire. Aux États-Unis, les autorités sont tenues de respecter certaines normes ou règles en matière de preuves pour obtenir l'accès aux communications électroniques stockées. Ainsi les autorités requérantes doivent présenter des faits classés par ordre chronologique et avancer des arguments raisonnables pour prouver que les enregistrements électroniques constituent des preuves matérielles déterminantes dans une enquête en cours. Il est nécessaire de démontrer qu'il existe des faits solides et

fiables, et non des soupçons, indiquant qu'une infraction a été commise par une ou plusieurs personnes et que le contenu du compte de courrier électronique ou du réseau social recèle des informations sur l'infraction faisant l'objet de l'enquête.

Dans le même ordre d'idées, la Direction nationale du renseignement assure, dans les deux sens, la coordination des enquêtes et des recherches menées sur demande des pays qui s'adressent directement à elle dans le cadre de la coopération internationale.

Coopération et assistance internationales visant à promouvoir la sécurité et le renforcement des capacités dans le domaine des technologies numériques

Pour la Colombie, la question du renforcement des capacités est fondamentale en matière de technologie.

La gestion des risques liés à la sécurité numérique est un domaine dans lequel les États, le secteur privé et les universités peuvent travailler ensemble, et des mécanismes de coopération et d'assistance internationales devraient être envisagés à cette fin.

Il importe d'associer les différentes parties prenantes à l'analyse de la question de la cybersécurité. Leur aide est très précieuse, tant pour établir un diagnostic que pour l'adoption de mesures de sécurité préventives et de mesures d'intervention en cas d'incident et d'urgence.

Il est important que les États commencent, en interne, par dresser la liste des domaines dans lesquels ils doivent renforcer leurs capacités. Pour ce faire, ils peuvent s'appuyer sur les modèles de maturité des capacités qui ont été élaborés au niveau international.

Il convient à partir de là de concevoir des plans de renforcement des capacités qui passent notamment par la mise en valeur des capacités opérationnelles, administratives, humaines, scientifiques et le développement des infrastructures physiques et technologiques, plans destinés aux organismes et entités responsables de la cybersécurité, ainsi qu'aux secteurs essentiels. De même, et dans le cadre de ce renforcement, il importe de mettre régulièrement à jour le catalogue des infrastructures cybernétiques critiques nationales et leurs plans de protection, ainsi que les mécanismes régissant la coordination entre elles.

Comme il s'agit d'une question qui nous concerne tous, il est essentiel de travailler à la création de contenus éducatifs portant sur la sécurité numérique, afin qu'ils puissent être inclus dans les programmes scolaires, tous niveaux d'enseignement confondus, ainsi que dans les cours non formels.

En ce qui concerne l'établissement de procédures d'entraide pour faire face aux incidents et aux problèmes de sécurité des réseaux à court terme, y compris de procédures d'accélération de l'assistance, la Colombie s'est dotée d'une procédure nationale d'intervention en cas d'incident où qu'il survienne sur le territoire national, en vertu de laquelle les instances compétentes agissent conformément à leurs pouvoirs et fonctions.

Ainsi, l'équipe d'intervention en cas d'atteinte à la sécurité informatique a été créée pour renforcer l'écosystème numérique au sein des entités publiques, en leur fournissant des services gratuits. Parmi les services fournis figurent des services proactifs, des services réactifs et des services de gestion de la sécurité, impliquant notamment le contrôle de la disponibilité des sites, l'analyse de la vulnérabilité, l'évaluation des problèmes de sécurité, un soutien dans la prise en charge et la riposte en cas d'incident, ainsi que la sensibilisation à la prise en charge des incidents.

L'équipe d'intervention collabore avec les autres instances publiques compétentes (le Groupe colombien d'intervention en cas d'atteinte à la sécurité informatique, le Commandement cybernétique conjoint des forces armées, le Centre cybernétique de la police), pour faire face aux incidents impliquant des entités de l'État et, par le biais du Comité de sécurité numérique, elle participe à l'élaboration de stratégies de gestion des questions touchant la sécurité numérique des citoyens, du secteur privé et de l'État.

Afin de faciliter la coopération transfrontière visant à pallier les vulnérabilités des infrastructures critiques qui dépassent les frontières nationales, le Bureau du Procureur élabore également avec les pays de la région des stratégies d'échange souple d'informations à jour en lien avec les enquêtes internes dans le cadre desquelles on sait qu'il existe un risque d'attaque ou d'atteinte aux infrastructures critiques.

Par l'intermédiaire de l'équipe d'intervention en cas d'atteinte à la sécurité nationale, le Ministère des technologies numériques coordonne son action avec le Groupe colombien d'intervention en cas d'atteinte à la sécurité informatique et le Centre cybernétique de la police pour valider les informations provenant de diverses sources internationales qui permettent de mener des actions d'atténuation et d'enquêter, le cas échéant.

En ce qui concerne l'élaboration de stratégies en faveur de la durabilité dans les initiatives de renforcement des capacités en matière de sécurité des technologies numériques, des lignes directrices et des recommandations pour le renforcement des capacités ont été incluses dans les différents instruments de politique publique contenus dans les documents 3711 et 3854 de 2016 du Conseil national de la politique économique et sociale. En outre, le Ministère des technologies numériques et le Ministère de la défense, entre autres, ont adopté d'autres mesures administratives et juridiques dans le but de renforcer la capacité de réaction.

À titre d'exemple, des accords de coopération ont été conclus entre le Gouvernement colombien et l'Organisation des États américains (OEA), en vertu desquels les parties conjuguent leurs efforts de coopération technique, afin de contribuer à la mise à jour des lignes directrices en matière de sécurité numérique ainsi qu'au renforcement des capacités et des compétences techniques pour la gestion des risques cybernétiques par des initiatives dans deux domaines fondamentaux : i) l'élaboration et la diffusion de politiques et ii) le renforcement des capacités.

Par l'intermédiaire de la Direction des affaires internationales, le Bureau du Procureur général a suivi les lignes directrices et les recommandations adoptées par les différentes instances multilatérales pour renforcer la sécurité dans le cyberespace, dans le but de garantir une bonne gestion des enquêtes sur la cybercriminalité et de réduire ainsi l'impunité dans toute la mesure du possible.

Afin de contribuer aux capacités nationales, la Direction nationale du renseignement a décidé de créer l'équipe d'intervention en cas d'atteinte à la sécurité informatique dans le domaine du renseignement. Il s'agit d'un mécanisme de coordination de la gestion des événements et incidents dans ce secteur, chargé d'organiser la diffusion d'informations techniques sur les événements et incidents, ainsi que d'enquêter sur les incidents cybernétiques.

La Colombie a aussi accordé la priorité à la sensibilisation à la sécurité des technologies numériques, ainsi qu'au renforcement des capacités dans les plans et budgets nationaux, l'objectif étant d'accorder à la sécurité l'importance qu'elle mérite dans la planification du développement et de l'aide. À cet égard, outre les politiques publiques en matière de sécurité numérique mentionnées plus haut, des programmes

de sensibilisation à la sécurité des technologies numériques ont été élaborés afin d'éduquer et d'informer les institutions et les citoyens.

Ainsi, le Ministère des technologies numériques s'est efforcé de mettre en place un programme axé sur le renforcement des capacités et, dans le cadre des accords de coopération conclus, il a organisé des cours et la délivrance de diplômes et de certificats en sécurité de l'information et en gestion informatique, dont ont bénéficié 1 134 fonctionnaires d'organismes gouvernementaux aux niveaux national et territorial.

Il convient ici de mentionner que, dans le cadre du programme « Parlons d'administration numérique », plus de 250 fonctionnaires des technologies numériques et agents de sécurité d'organismes publics ont participé à la réunion-débat consacrée au renforcement des capacités de gestion de la sécurité et des risques numériques.

Un cyberdéfi a été lancé aux fonctionnaires dans la ville de Pereira, auquel ont pris part 40 dirigeants du secteur des technologies numériques. Ils ont également participé à un défi sur la cybersécurité, dans le cadre duquel ils se sont affrontés autour de problèmes et de situations pouvant survenir en ligne. Cet évènement a été organisé par l'OEA, avec le soutien de Trend Micro, une multinationale spécialisée dans la cybersécurité.

Dans le cadre des ateliers consacrés à l'amélioration de la sécurité pour améliorer la région, plus de 1 400 fonctionnaires ont pris part aux 25 rencontres organisées dans 24 villes de Colombie, notamment des responsables des technologies numériques et des agents de sécurité d'organismes publics.

Avec le soutien de l'OEA, il a été possible de renforcer les processus de formation dans la région. À titre d'exemple, le cours consacré au « Processus de La Haye : opérations de sécurité internationales et cyberespace », financé par le Royaume des Pays-Bas, a été organisé à plusieurs reprises. En 2019, il a eu lieu en Colombie et, outre la formation dispensée aux fonctionnaires colombiens, des représentants d'Amérique latine et des Caraïbes ayant des compétences en matière de cybersécurité y ont également participé. Le cours porte sur des sujets tels que la souveraineté, la compétence, le principe de diligence raisonnable, l'emploi de la force, le droit international des droits de l'homme, le droit de la mer et le règlement pacifique des différends, entre autres, le tout abordé sous un angle académique et par l'étude d'opérations cybernétiques.

En ce qui concerne le renforcement des capacités en criminalistique ou en matière de coopération visant à faire face à l'utilisation des technologies numériques à des fins terroristes ou criminelles, le Gouvernement colombien a accueilli un atelier régional pour l'Amérique latine sur l'obtention de preuves électroniques auprès des fournisseurs de services de communication privés dans le cadre de la lutte contre le terrorisme et la criminalité organisée, en lien avec des enquêtes transfrontières, organisé par l'OEA ; la Direction exécutive du Comité contre le terrorisme de l'Organisation des Nations Unies ; l'Office des Nations Unies contre la drogue et le crime ; l'Association internationale des procureurs et poursuivants, la Coordination nationale de la sécurité numérique et le Ministère colombien des technologies numériques. Des représentants de 13 pays d'Amérique latine (fonctionnaires de police judiciaire et d'autres services publics) ont participé à une formation sur l'obtention de preuves numériques transfrontières ; l'évolution de la législation aux États-Unis, au Canada et dans l'Union européenne ; les demandes de divulgation d'urgence et la rédaction de demandes d'entraide judiciaire, entre autres, dans le but de renforcer la coopération internationale en matière de lutte contre le terrorisme et la criminalité organisée.

Ces trois dernières années, le Bureau du Procureur général a autorisé l'envoi d'officiers de police judiciaire affectés aux groupes délits informatiques et criminalistique informatique qui ont participé à d'importants séminaires ou formations organisés par l'OEA et le Registre d'adresses Internet pour l'Amérique latine et les Caraïbes, entre autres ; ainsi que de procureurs qui connaissent et dirigent des enquêtes en lien avec la technologie (comme fin ou comme moyen de commettre un crime).

Par ailleurs, avec le soutien d'entités privées et d'universités locales, divers cours de formation ont été organisés sur la lutte contre la cybercriminalité et l'amélioration des techniques et la formation au matériel et aux logiciels d'analyse des preuves numériques aux fins du recoupement entre les affaires et de la détection de tendances.

En coordination avec l'équipe d'intervention compétente en cas d'atteinte à la sécurité, la Direction nationale du renseignement, prévoit de créer des capacités en matière de détection des intrusions informatiques et d'analyse de la vulnérabilité, d'analyse criminalistique et de récupération des données numériques, d'analyse des logiciels malveillants et des artéfacts numériques, d'analyse des applications, en lien avec le laboratoire *open source* et l'étude des phénomènes survenant dans le cyberespace.

En réponse à la recommandation d'opter pour une approche régionale du renforcement des capacités, en tenant compte des particularités culturelles, géographiques, politiques, économiques ou sociales, afin de promouvoir une gestion au cas par cas, le Ministère des technologies numériques, agissant par l'intermédiaire du groupe chargé de la sécurité et de la confidentialité de la Direction de la gouvernance numérique, a mis en œuvre un modèle de sécurité et de confidentialité de l'information. Celui-ci englobe les instruments qui permettent aux instances nationales et territoriales de faire face aux cybermenaces, en instaurant une culture de la sécurité à même de faire connaître les cybermenaces qui affectent les organisations au niveau transnational.

En outre, les autorités chargées de la politique pénale sont en train d'élaborer un plan national englobant diverses formes de criminalité.

La Direction nationale du renseignement travaille à la création d'un dispositif d'échange d'informations sécurisé destiné aux professionnels nationaux du renseignement. Dans le même ordre d'idées, un projet est en cours d'élaboration qui porte sur la formation et le renforcement des capacités de protection et de gestion des bonnes pratiques pour les pays des Caraïbes, en coordination avec l'Agence présidentielle de coopération.

Dans le but de renforcer les capacités en matière de sécurité des technologies numériques, et comme nous l'avons déjà indiqué, la Colombie a pris part à des initiatives de coopération bilatérale et multilatérale, afin d'améliorer les conditions d'une entraide efficace visant à faire face aux incidents liés aux technologies numériques.

Ainsi, le Ministère des technologies numériques est aussi en train d'élaborer des stratégies de coopération avec les entreprises de sécurité et les instances internationales compétentes, l'objectif étant de partager les renseignements disponibles en lien avec des menaces stratégiques, tactiques et opérationnelles.

Application du droit international à l'utilisation des technologies numériques

La Colombie considère que le droit international, en particulier la Charte des Nations Unies et notamment le droit international des droits de l'homme et le droit

international humanitaire, s'applique au monde « virtuel » aussi bien qu'au monde « physique ».

Nous sommes d'accord avec le Secrétaire général, qui disait dans l'avant-propos du rapport établi en 2015 par le Groupe d'experts gouvernementaux : « Le cyberespace ne peut devenir un environnement stable et sûr que grâce à la coopération internationale, et le droit international et les principes de la Charte des Nations Unies doivent être à la base de cette coopération. »

C'est pourquoi la Colombie considère que les principes généraux du droit international peuvent s'appliquer dans le cyberespace, moyennant les ajustements nécessaires qu'exigent les opérations virtuelles et leurs particularités.

Étant donné les interprétations possibles de certains éléments du droit international dans le cyberespace, nous n'excluons pas la possibilité d'élaborer des guides ou des manuels pour orienter l'application du droit international public dans le cyberespace.

À cet égard, la Convention sur la cybercriminalité (Budapest, 2001) pourrait être utile, au regard des notes d'orientation qui l'accompagnent pour guider la mise en œuvre de ses dispositions et les adapter aux progrès de la technique. Elle est considérée comme une bonne pratique qui pourrait être imitée.

Considérant que l'Assemblée générale des Nations Unies a recommandé et accueilli favorablement l'ensemble des règles, normes et principes internationaux de comportement responsable des États consacrés dans les rapports des groupes d'experts gouvernementaux, pour la Colombie, il convient de faire mieux appliquer immédiatement ces normes. Un instrument juridiquement contraignant n'a pour l'instant pas lieu d'être.

De même, il convient de souligner que la Colombie est respectueuse des engagements contractés et des garanties données.

Concepts

Il faudra continuer d'examiner, dans le cadre des instances multilatérales, le développement conceptuel que l'on a jugé nécessaire de promouvoir pour bien cerner les concepts liés à la paix et à la sécurité internationales et l'utilisation des technologies numériques aux niveaux juridique, technique et politique, compte tenu des particularités et de la nouveauté qui caractérisent ces questions.

Ces discussions sont essentielles pour adapter les normes internationales aux défis du cyberespace et dégager un consensus sur la façon d'appliquer le droit international dans cet espace virtuel. À cet égard, la Colombie partage les conclusions formulées par le Groupe d'experts gouvernementaux dans son rapport de 2015 et est prête à approfondir les discussions avec d'autres délégations sous l'égide de l'Organisation des Nations Unies.

Ce n'est qu'ainsi que l'on pourra garantir une utilisation appropriée des technologies numériques, qui sont essentielles pour relever les défis auxquels la communauté internationale est actuellement confrontée, et empêcher qu'elles ne soient utilisées d'une manière contraire aux objectifs et aux buts énoncés dans la Charte des Nations Unies, en garantissant pleinement la paix et de la sécurité internationales.

Les nouvelles technologies, véhicule novateur de prestation de services, ouvrent de nouvelles possibilités dans la société de l'information ; elles reposent sur un traitement sécurisé de l'information et sur la protection spéciale des données

personnelles, ce qui permet de tirer parti des avancées technologiques et d'en améliorer la contribution au développement social et économique.

Pour les raisons susmentionnées, il faut absolument que les gouvernements se mobilisent davantage pour s'entendre sur une nouvelle approche qui fasse fond sur les meilleures pratiques internationales face aux risques liés à la sécurité numérique, en tenant compte des principes qui régissent le comportement responsable des États, qui permettent d'accéder aux forums de discussion internationaux sur la sécurité numérique et d'adopter une conduite transparente et prévisible, réduisant ainsi tout risque de malentendu, d'escalade et de conflit en matière de sécurité numérique.

Enfin, les stratégies appliquées et les actions posées en faveur d'une utilisation responsable de l'environnement numérique contribuent à l'édification de la paix grâce à la création de conditions propices à la cohabitation numérique basée sur le respect, en soutenant la liberté d'expression et l'emploi d'un langage approprié en ligne, en réfléchissant au moyen de tirer parti des avantages offerts par les technologies numériques et en soutenant l'adaptation pour l'avenir numérique.

Danemark

[Original : anglais]
[29 mai 2020]

À l'instar du reste du monde, le Danemark est de plus en plus connecté grâce à Internet. Les solutions numériques font partie du quotidien et contribuent à la croissance économique. Pays parmi les plus numérisés au monde, le Danemark considère qu'il est d'une importance vitale de promouvoir un cyberespace mondial ouvert, stable, pacifique et sûr au sein duquel les droits de la personne, les libertés fondamentales et l'État de droit s'appliqueraient intégralement.

Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

Le Danemark a adopté plusieurs mesures afin de renforcer sa sécurité informatique et de promouvoir la coopération internationale dans le cyberespace.

L'Accord sur la défense pour la période 2018-2023 prévoit l'allocation de 1,4 milliard de couronnes danoises pour renforcer la cybersécurité et la cyberdéfense et, ce faisant, accroître la résilience du pays. La Stratégie danoise sur la cybersécurité et la sécurité de l'information 2018-2021 prévoit des mesures supplémentaires afin de renforcer la cybersécurité. Grâce à 25 initiatives et 6 stratégies ciblées dans les domaines considérés essentiels (énergie, finance, transport, soins de santé, télécommunications et secteur maritime), le Danemark a renforcé la résilience technologique de ses infrastructures, développé les connaissances et compétences des citoyens, des entreprises et des autorités et intensifié la coordination et la coopération dans le domaine de la cybersécurité. En outre, la Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne a été pleinement incorporée à la législation danoise.

Dans le cadre de la Stratégie sur la cybersécurité et la sécurité de l'information 2018-2021, des unités de sécurité informatique et de cybersécurité ont été mises sur pied dans les six secteurs susmentionnés. La Stratégie prévoit également la création d'une plateforme rassemblant ces unités sectorielles ainsi que le Centre pour la cybersécurité. Cette plateforme leur permet de procéder à un partage d'expérience en matière de cybersécurité et de sécurité de l'information. L'Agence danoise de la

numérisation et les Services de sécurité et de renseignement danois participent également aux travaux de cette plateforme.

Afin de disposer d'un personnel suffisamment qualifié pour identifier et gérer les cyberattaques perpétrées contre le Danemark, et en particulier contre ses infrastructures critiques, le Centre pour la cybersécurité a créé et mis sur pied sa propre Cyberacadémie proposant une formation intensive. En 2019, 15 personnes ont suivi la formation et sont désormais employées au centre d'opérations du Centre. Parallèlement, le Centre appuie également la recherche et la formation en matière de cybersécurité. Par exemple, en 2019, il a collaboré avec la Faculté de conception et de technologies de Copenhague, l'Université d'Aalborg, l'Université du Sud du Danemark, la Faculté de commerce de Copenhague et l'Université technique du Danemark à l'organisation des tout premiers cours d'été sur la cybersécurité .

En 2019, un Conseil de cybersécurité (Cybersikkerhedsråd), qui rassemble des entités publiques et privées, a été créé afin d'offrir les qualifications nécessaires aux pouvoirs publics et au secteur privé, de renforcer la démocratie numérique et de sensibiliser aux menaces et possibilités découlant de la numérisation et des nouvelles technologies.

Dans le cadre de la Stratégie danoise sur la cybersécurité et la sécurité de l'information 2018-2021, le Danemark a détaché des chargés de la cybersécurité à Bruxelles ; il a désigné un coordinateur international pour le numérique au Ministère des affaires étrangères ; il a nommé un conseiller à la cybersécurité au Bureau de l'Ambassadeur des technologies dans la Silicon Valley ; il a adhéré au Centre coopératif d'excellence sur la cyberdéfense de l'Organisation du Traité de l'Atlantique Nord à Tallinn. Ce faisant, il a renforcé sa présence internationale en matière de cybersécurité. Cela lui a également permis de participer plus avant aux travaux sur la cybersécurité d'organisations internationales, telles que l'ONU, l'Union européenne, l'Organisation du Traité de l'Atlantique Nord et l'Organisation pour la sécurité et la coopération en Europe. Le Danemark est également un membre actif du Groupe de coopération pour la sécurité des réseaux et de l'information et du Réseau d'équipes d'intervention en cas d'atteinte à la sécurité informatique. Il fait aussi partie du Conseil d'administration de l'Agence de l'Union européenne pour la cybersécurité. En participant à ces instances, le Danemark n'a eu de cesse de promouvoir un cyberespace mondial ouvert, stable, pacifique et sûr.

De plus, le Danemark a joué un rôle actif dans l'élaboration de la boîte à outils de l'Union européenne pour la sécurité des réseaux 5G. Celle-ci a pour but de coordonner l'approche européenne eu égard à la 5G sur la base d'un ensemble de mesures communes visant à atténuer les principaux risques en matière de cybersécurité associés à ces réseaux.

Le Danemark souscrit au message clair envoyé par la communauté internationale et souligne que le cyberespace est profondément ancré dans le droit international existant, comme indiqué par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale dans ses rapports de 2013 et 2015, adoptés par consensus. Le droit international existant, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme s'appliquent pleinement au comportement des États dans le cyberespace. Le Danemark met en outre en exergue l'importance des 11 normes facultatives et non contraignantes de comportement responsable des États énoncées dans le rapport du Groupe d'experts gouvernementaux, qui viennent compléter les dispositions contraignantes du droit international.

Malgré nos efforts, la capacité et la volonté d'acteurs étatiques et non étatiques de mener des activités malveillantes dans le cyberespace ne faiblissent pas. Il devrait s'agir d'une source de préoccupation mondiale. Ces activités malveillantes peuvent en effet constituer des actes répréhensibles au sens du droit international et être source de déstabilisation et d'escalade. Le Danemark demeure déterminé à prévenir, dissuader et combattre ces activités malveillantes et entend renforcer la coopération internationale à cette fin. Il souscrit à l'appel que l'Union européenne a lancé à la communauté internationale l'invitant à renforcer la coopération internationale en faveur d'un cyberespace mondial ouvert, stable, pacifique et sûr, où s'appliquent intégralement les droits de l'homme, les libertés fondamentales et l'État de droit.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Menaces existantes et émergentes

Comme indiqué précédemment, le Danemark reconnait que le cyberespace offre des possibilités majeures d'accroître le bien-être, de stimuler la croissance économique et d'améliorer la qualité de vie de la population. Toutefois, notre dépendance vis-à-vis des solutions numériques n'est pas dénuée de risques.

Le Danemark est préoccupé par l'augmentation du nombre d'attaques malveillantes commises par des acteurs étatiques et non étatiques dans le cyberespace ; il est également préoccupé par l'utilisation qui est faite du cyberespace pour violer les droits de propriété intellectuelle. Ces agissements menacent la croissance économique et la stabilité de la communauté internationale.

L'importance d'un cyberespace ouvert, sûr, stable, accessible et pacifique n'a jamais été aussi marquée qu'à l'heure de la pandémie de maladie à coronavirus (COVID-19). Les technologies numériques permettent de communiquer, de collaborer et de procéder à un partage d'expérience, ce qui est essentiel afin de lutter à l'échelle mondiale contre la pandémie.

Cependant, la crise liée à la COVID-19 nous a montré que des acteurs mal intentionnés sont prêts à tirer parti de toute occasion, y compris d'une pandémie. Ils sont même prêts à porter atteinte aux infrastructures critiques, y compris les hôpitaux, qui sont essentiels à la lutte contre la pandémie. Ces agissements sont inacceptables et doivent être condamnés dans les termes les plus forts par tous les États. En outre, ceux-ci doivent faire preuve de la diligence requise et lutter fermement et sans attendre contre toute utilisation malveillante des technologies numériques émanant de leur territoire.

Application du droit international aux technologies numériques

Le Danemark est très favorable à un système multilatéral basé sur un ordre international fondé sur des règles, qui permette de s'attaquer aux menaces existantes et éventuelles découlant de l'utilisation des technologies numériques à des fins malveillantes.

La communauté internationale a fait clairement savoir que le cyberespace était fermement ancré dans le droit international existant, comme en attestent également les rapports consensuels du Groupe d'experts gouvernementaux de 2013 et 2015. Le Danemark souligne que le droit international existant, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme s'appliquent au comportement des États dans le cyberespace.

La souveraineté, la non-ingérence et la prohibition du recours à la force constituent les principes fondamentaux du droit international. La violation de ces

principes constitue un fait internationalement illicite passible de contremesures, pour lequel les États peuvent chercher à obtenir réparation en vertu des dispositions qui régissent la responsabilité de l'État. Il demeure possible de dégager une conception et une interprétation communes de ces principes, et le Danemark appuie le travail fait en ce sens par le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, ainsi que dans le cadre d'autres initiatives internationales et régionales.

Il est important que le principe de souveraineté ne soit pas utilisé par les États pour restreindre ou violer le droit international des droits de l'homme à l'intérieur de leurs propres frontières. Les droits de l'homme sont applicables en ligne et hors-ligne. À ce titre, les États ont à la fois des obligations positives et négatives et doivent s'abstenir de violer les droits de l'homme tout en s'assurant que chacun et chacune puisse jouir de ses droits et libertés.

Comme indiqué dans le Manuel militaire danois, les opérations dans le cyberespace ne diffèrent pas des capacités militaires traditionnelles du point de vue de l'applicabilité du droit international. La question a également été abordée dans le cadre de la *Doctrine conjointe pour les opérations militaires dans le cyberespace* de 2019, qui prévoit que les responsables de l'armée soient guidés par le respect du droit international lors d'opérations dans le cyberespace. Par conséquent, le droit international humanitaire, y compris les principes de précaution, d'humanité, de nécessité militaire, de proportionnalité et de distinction, s'applique à la conduite des États dans le cyberespace. Ces principes constituent également un cadre transversal de protection qui définit les limites de la licéité de la conduite des États en temps de conflit armé. Le Danemark s'associe à l'Union européenne et souligne que le droit international n'encourage pas les conflits, mais vise plutôt à protéger les civils et à limiter les effets excessifs des conflits.

Le droit international existant, complété par les 11 normes facultatives et non contraignantes de comportement responsable des États énoncées dans le rapport du Groupe d'experts gouvernementaux de 2015, constitue un cadre de comportement responsable dans le cyberespace. Le Danemark appelle tous les États à le respecter et à mettre en œuvre les recommandations qui en découlent.

Puisqu'il existe déjà un cadre juridique international concernant les questions relatives au cyberespace, le Danemark n'est pas favorable à l'élaboration de nouveaux instruments juridiques internationaux à ce sujet et n'en voit pas la nécessité. Il demeure toutefois possible de parvenir à une interprétation commune de la manière dont ce cadre s'applique. Le Danemark espère que les recommandations du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée contribueront à préciser l'applicabilité de ce cadre et à en favoriser le respect par les États. À terme, cela permettra d'assurer une plus grande prévisibilité et de réduire les risques d'escalade.

Normes, règles et principes de comportement responsable des États

À l'instar de l'Union européenne et de ses États membres, le Danemark encourage tous les États à faire fond sur les documents adoptés par l'Assemblée générale, en particulier la résolution 70/237, à faire avancer ce travail et à appliquer les normes et mesures de confiance convenues, qui jouent un rôle crucial dans la prévention des conflits.

Les normes, règles et principes de comportement responsable des États, qui sont énoncés dans les rapports successifs du Groupe d'experts gouvernementaux de 2010, 2013 et 2015 et qui viennent compléter le droit international contraignant, ont une

valeur inestimable. Le Danemark demeurera guidé par le droit international et par le respect volontaire de ces normes, règles et principes. Ces normes devraient être mises en œuvre par le biais d'un renforcement de la coopération et de la transparence et dans le cadre de bonnes pratiques.

Émirats arabes unis

[Original : arabe]
[31 mai 2020]

Rapport national sur les mesures prises par les Émirats arabes unis pour renforcer la sécurité de l'information et promouvoir la coopération internationale en matière de cybersécurité

Introduction

Les Émirats arabes unis attachent une grande importance à la cybersécurité qui est essentielle pour maintenir la sécurité nationale, face aux attaques menées à l'aide des technologies numériques, qui mettent gravement en péril les infrastructures, les services publics et les personnes. Les Émirats arabes unis se sont donc efforcés d'instaurer un système intégré pour garantir la sécurité des secteurs vitaux, renforcer la confiance des usagers et stimuler l'innovation.

Mesures prises au niveau national pour renforcer la cybersécurité

Le pays a lancé une stratégie nationale de cybersécurité, visant à créer un environnement numérique sûr et flexible et à permettre aux personnes de réaliser leurs ambitions et aux entreprises de se développer, avec les cinq objectifs suivants :

1. Mettre en place un cadre juridique et réglementaire complet pour lutter contre la cybercriminalité, protéger les technologies actuelles ou nouvelles et permettre aux petites et moyennes entreprises de se prémunir contre les cybermenaces ;

2. Élaborer un programme intégré de sensibilisation et de renforcement des capacités dans le domaine de la cybersécurité, en vue d'encourager des pratiques sûres sur le plan de l'utilisation des technologies et de renforcer les compétences du personnel chargé de la cybersécurité afin qu'il puisse efficacement repousser les attaques et sécuriser les systèmes et les services ;

3. Mettre en place un plan national efficace pour intervenir de manière rapide et coordonnée dans le pays, à la suite des atteintes à la cybersécurité ;

4. Protéger les infrastructures numériques dans les secteurs vitaux ;

5. Renforcer les partenariats locaux et mondiaux en matière de cybersécurité.

En 2006, les Émirats arabes unis ont adopté une loi pour réprimer les infractions liées aux technologies numériques, qui comprend bon nombre de dispositions visant à protéger le contenu privé, qui a été publié et diffusé sur des supports numériques, et à sanctionner l'utilisation de ces supports à des fins illicites.

Les Émirats arabes unis ont également lancé bon nombre de programmes et d'initiatives au fil des ans pour renforcer la cybersécurité et ont établi notamment une équipe d'intervention en cas d'atteinte à la sécurité informatique, qui dispense tout un éventail de services aux organismes publics, tels que : la surveillance et l'inspection en continu des infrastructures afin de détecter toute activité ou attaque inhabituelle et d'y répondre ; l'intervention efficace en cas d'atteinte à la cybersécurité ; et l'évaluation de la sécurité des sites Web et des applications de téléphonie mobile afin de remédier aux faiblesses pouvant être exploitées ou entraîner

la fuite d'informations. L'équipe fournit également aux organismes publics et aux particuliers, par l'intermédiaire de diverses plateformes, dont son site Web, et des médias sociaux, une liste de diffusion, des avis de sécurité réguliers et des comptes rendus sur les cyberattaques majeures.

Pour veiller à faire appliquer les meilleures pratiques de cybersécurité dans tous les secteurs vitaux du pays, un système visant à garantir la sécurité de l'information a été mis en place afin de servir de critère, de relever le niveau de protection minimum des informations et d'en assurer la sécurité, à l'aide de systèmes de soutien.

Outre les politiques et les systèmes techniques, il a fallu renforcer les compétences du personnel afin de le sensibiliser à l'utilisation constructive et sûre des technologies numériques et d'en faire la première ligne de défense contre les dangers des cyberattaques, tant pour le pays que pour les familles. Un programme national de sensibilisation à la cybersécurité et de renforcement des capacités a donc été lancé pour favoriser une culture de la cybersécurité dans la société et développer des compétences nationales en la matière. Dans le cadre de l'initiative CyberPro, des spécialistes de la cybersécurité suivent des cours mensuels. Une académie virtuelle proposant des formations dans le même domaine a également été créée et des campagnes d'information et des événements publics sont organisés périodiquement à l'intention des divers segments de la société.

Le personnage de bande dessinée Salim, créé aux fins de la protection des enfants en ligne, a fait de grands progrès pour communiquer, de manière ludique et simple, les principes d'une utilisation sûre de la technologie. Outre le programme de sécurité numérique établi en coopération avec le Ministère de l'éducation et le lancement du site Web Salim, des milliers d'ateliers interactifs ont été organisés pour éduquer les enfants au moyen de récits dont ils sont les protagonistes. Ces initiatives ont également conduit à la participation des enfants à la sensibilisation par l'intermédiaire de l'initiative des ambassadeurs de la cybersécurité, qui leur donne les outils nécessaires pour sensibiliser leurs pairs et encourager un moyen sûr et sain d'aborder le sujet.

Mesures visant à renforcer la coopération en matière de cybersécurité

Les Émirats arabes unis savent bien que pour atteindre un niveau optimal de cybersécurité et de capacité de réponse aux attaques et aux risques, il faut une coopération internationale. Ils s'efforcent donc de participer activement à tous les forums internationaux sur la cybersécurité, dont certains sont mentionnés ci-dessous.

Les Émirats arabes unis sont membres de l'Union internationale des télécommunications (UIT) et coopèrent avec les autres États membres pour trouver des solutions et répertorier les meilleures pratiques en matière de cybersécurité par l'intermédiaire des commissions d'étude et des groupes de travail compétents. Certains de leurs propres spécialistes occupent des postes clefs au sein de l'Union, comme le chef du Groupe de travail du Conseil de l'UIT sur la protection des enfants en ligne, ce qui montre combien le pays s'attache à soutenir les efforts mondiaux sur ces questions importantes.

Les Émirats arabes unis sont représentés au sein de l'équipe d'intervention en cas d'atteinte à la sécurité informatique du Conseil d'administration de l'Organisation de la coopération islamique, dans laquelle ils encouragent la sensibilisation à la cybersécurité en élaborant des programmes, des manuels et autre matériel essentiel sur les risques de sécurité pour les institutions et les individus. L'équipe d'intervention en cas d'atteinte à la sécurité informatique des Émirats arabes unis prend également une part active au Centre régional arabe pour la cybersécurité et au

Comité des centres nationaux d'intervention d'urgence informatique du Conseil de coopération du Golfe.

Outre le fait de collaborer avec des forums et des organisations internationales, les Émirats arabes unis souhaitent renforcer la coopération bilatérale en matière de cybersécurité avec les pays amis en signant des mémorandums et des protocoles d'accord pour réglementer l'échange d'informations et de compétences et la coopération entre les pays, face aux cyberattaques.

Vues relatives aux notions évoquées dans les rapports du Groupe d'experts gouvernementaux

Les Émirats arabes unis souhaitent remercier le Groupe d'experts gouvernementaux pour ses rapports sur les faits nouveaux intervenus sur le plan du numérique dans le cadre de la sécurité internationale. Ils approuvent les conclusions du Groupe sur l'importance pour les États de s'efforcer de prévenir les pratiques préjudiciables en matière de technologies numériques, de coopérer pour répondre aux cyberattaques, de soutenir un dialogue fondé sur la transparence et l'action conjointe, d'appuyer le renforcement mondial des infrastructures numériques et de se concerter sur l'élaboration de lois, de stratégies et de systèmes de cybersécurité.

France

[Original : français]
[29 mai 2020]

La France salue l'opportunité qui lui est offerte de répondre à la résolution 74/28 de l'Assemblée générale des Nations Unies intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » et souhaite apporter les précisions suivantes.

1. Appréciation générale des problématiques de cybersécurité

À titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information », auquel elle préfère le terme de « sécurité des systèmes d'information » ou encore « cybersécurité ». La France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité. Par ailleurs, le terme de « cybersécurité » est ainsi plus précis, en ce qu'il désigne la capacité d'un système d'information de résister à des événements issus du cyberespace et susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La France considère que l'espace numérique doit rester un espace de liberté, d'échange et de croissance, qui contribue à la prospérité et au progrès dans nos sociétés**.** Ce cyberespace ouvert, sûr, stable, accessible et pacifique, porteur d'opportunités économiques, politiques, sociales, promu par la France au cours des trois dernières décennies, est aujourd'hui menacé par de nouvelles pratiques malveillantes qui se développent dans le cyberespace. En effet, les spécificités de l'espace numérique (relatif anonymat, faiblesse des coûts et facilité d'accès aux outils malveillants, existence de vulnérabilités, prolifération de certains outils, etc.) permettent à nombre d'acteurs de mener des actions d'espionnage, de trafics illicites, de déstabilisation et de sabotage. Si certaines menaces de faible intensité ne relèvent pas de la sécurité nationale, mais constituent plutôt une forme de criminalité, l'utilisation de ces outils visant des systèmes informatiques d'État, des infrastructures critiques ou des entreprises peut avoir de graves conséquences.

Les enjeux de cybersécurité font désormais partie intégrante des stratégies de puissance et des rapports de force qui régissent les relations internationales ; il s'agit là d'une priorité et d'un enjeu politique de premier ordre. La France estime que les États doivent conserver le monopole de la violence légitime, dans le cyberespace comme dans les autres domaines. Cependant, l'essor du numérique comme nouvel outil et espace de confrontation confère au secteur privé, notamment à un certain nombre d'acteurs systémiques, un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité internationales.

2. Efforts de la France en matière de cybersécurité aux niveaux national et international et vues de la France sur la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Afin de préserver, développer et promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique et de faire face aux menaces qui affectent la stabilité et la sécurité internationales, la France mène depuis plusieurs années une politique et une diplomatie active.

Les travaux des cinq premiers Groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, auxquels la France a participé, ont permis de réaliser des progrès dans la définition de principes communs et dans l'appréhension collective du cyberespace, notamment en matière de coopération internationale, de normes et de compréhension de l'application du droit international.

Actions de la France en matière de coopération internationale, de renforcement capacitaire et pour la promotion et le développement de mesures de confiance

L'action de la France en matière de promotion de la coopération internationale sur les enjeux de cybersécurité se décline dans un cadre bilatéral, européen et international.

Au niveau de l'Union européenne, dans le but de renforcer la cyberrésilience de l'espace européen, la France contribue au développement d'un cadre volontaire de coopération pour la prévention et la résolution des incidents. Il repose en particulier sur le développement de normes opérationnelles communes et de procédures de coopération entre partenaires, qui sont testées lors d'exercices paneuropéens. La France a également participé à l'élaboration d'une « boîte à outils cyber » offrant un cadre européen de réponse diplomatique conjointe à une attaque informatique, et reposant sur l'utilisation de mesures de prévention, de coopération, de stabilisation et de réponse (mesures restrictives notamment) aux incidents cyber. Elle participe également au développement du réseau CyCLONe qui permet d'organiser la coopération opérationnelle entre agences nationales de cybersécurité européennes en cas de crises cyber et à l'organisation d'exercices conjoints pour s'y préparer en complément de la coopération entre leurs centres de veille, d'alerte et de réponse aux attaques informatiques.

Au sein de l'Organisation du Traité de l'Atlantique Nord (OTAN), la France a été à l'initiative de l'adoption par les alliés d'un engagement en faveur de la cyberdéfense, lors du Sommet de Varsovie en juin 2016. Cet engagement permet de s'assurer que chaque État membre de l'OTAN consacre une part appropriée de ses ressources au renforcement de ses capacités de cyberdéfense, permettant ainsi d'élever le niveau de sécurité général de l'Alliance.

Participant activement au groupe de travail informel de l'Organisation pour la sécurité et la coopération en Europe (OSCE) sur la cybersécurité, la France continue de promouvoir la mise en œuvre des 16 mesures de confiance développées par l'OSCE

sur les enjeux dans ce domaine. Elle y pilote notamment, aux côtés d'autres États participants, la mise en œuvre d'une mesure de confiance sur la sécurisation des infrastructures critiques.

La France considère aussi que de nombreux enjeux liés à la cybersécurité méritent d'être abordés selon une approche multipartite, afin de prendre en compte le rôle et les responsabilités spécifiques d'acteurs non étatiques. Dans l'Appel de Paris, la France a souligné dès 2018 « la nécessité d'une approche multiacteur renforcée ». La France considère en effet que la société civile, le monde académique, le secteur privé et la communauté technique disposent de compétences et de ressources utiles à la définition de certains aspects des politiques pertinentes en matière de cybersécurité. Présenté par le Président de la République à l'occasion du Forum sur la gouvernance d'Internet, tenu à l'Organisation des Nations Unies pour l'éducation, la science et la culture le 12 novembre 2018, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace[2] témoigne ainsi du rôle actif joué par la France dans la promotion d'un cyberespace sûr, stable et ouvert. Initiative multiacteur la plus large au monde en matière de cybersécurité, l'Appel de Paris est soutenu à ce jour par 78 États et plus de 1 000 entités non étatiques. Il vise à promouvoir certains principes fondamentaux de la régulation de l'espace numérique, comme l'application du droit international et des droits de l'homme dans le cyberespace, le comportement responsable des États, le monopole étatique de la violence légitime ou encore la reconnaissance des responsabilités spécifiques des acteurs privés.

La France a également soutenu les activités de la Commission mondiale sur la stabilité du cyberespace, qui a travaillé à l'élaboration de propositions de normes et de politiques destinées à renforcer la sécurité et la stabilité internationales et à orienter le comportement responsable des États dans le cyberespace. Le rapport réunissant ses conclusions a été présenté lors du second Forum de Paris sur la Paix.

Au sein du Groupe des Vingt (G20), la France œuvre pour que les travaux portent sur les questions fondamentales de la concurrence dans l'économie numérique ou encore sur les nouveaux modes de régulation et de gouvernance de la sécurité numérique, dans la lignée de l'Appel de Paris.

Enfin, la France s'est également investie au sein de l'Organisation de coopération et de développement économiques (OCDE). Aujourd'hui, elle préside le Groupe de travail de l'OCDE sur la sécurité et la vie privée dans l'économie numérique et souhaite travailler sur des thèmes comme la responsabilité des acteurs privés, la sécurisation des produits et services, et la divulgation responsable des vulnérabilités.

En matière de renforcement capacitaire, en raison de la grande interconnexion des réseaux et sociétés, la France estime que la cybersécurité de tous ne sera assurée que lorsque chaque État se sera doté de capacités suffisantes pour sécuriser ses propres systèmes d'information. Dès lors, elle s'investit pour renforcer les capacités de cybersécurité de ses partenaires, à titre bilatéral ou dans le cadre d'initiatives multilatérales. Un tel investissement dans la coopération est, du reste, bénéfique pour toutes les parties : il permet de maintenir des connaissances de pointe en se confrontant à nos pairs et en apprenant d'eux, un enrichissement mutuel des savoirs et savoir-faire et le développement de la confiance entre les acteurs concernés. Au cours des dernières années, la France a également déployé au sein des forces de sécurité intérieure de pays partenaires des experts techniques internationaux en cybersécurité. La France poursuit par exemple avec le Sénégal des activités de l'école nationale à vocation régionale de cybersécurité de Dakar, inaugurée fin 2018. Ce

[2] Disponible à l'adresse suivante : https://pariscall.international/fr.

projet vise à fournir des formations courtes et adaptables pour des professionnels de la cybersécurité et des hauts fonctionnaires issus de l'Afrique de l'Ouest en priorité.

La définition de normes de comportement responsable, l'un des acquis importants

La France a mis en place un ensemble de dispositifs, à travers des éléments de doctrine nationale, de gouvernance et de législation permettant d'appliquer les normes de comportement agréées par les rapports du Groupe d'experts gouvernementaux , notamment le rapport de 2015 (A/70/174). Les éléments ci-après ont vocation à illustrer la manière dont la France a cherché à mettre en œuvre ces normes, mais ne visent pas à l'exhaustivité.

> Norme a : Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des technologies de l'information et des communications (TIC) et à prévenir les pratiques informatiques jugées nocives qui peuvent compromettre la paix et la sécurité internationales.

La France a pris un ensemble de mesures afin de répondre à cette norme notamment en consolidant une stratégie nationale de cybersécurité centrée sur la défense, la prévention, la résilience et la coopération. La revue stratégique de cybersécurité, publiée en 2018[3], définit une doctrine de gestion de crise et clarifie nos objectifs. Elle confirme le modèle français qui distingue les institutions responsables des capacités offensives de celles qui exercent des missions défensives. Cette revue affirme aussi fermement l'objectif diplomatique de développer la confiance et la stabilité dans le cyberespace.

La France met par ailleurs en place des dialogues stratégiques bilatéraux sur les questions de cybersécurité avec différentes partenaires. Elle est également active dans de nombreuses enceintes permettant une coopération et une coordination régionale et internationale, comme évoqué plus haut.

La France a également reconnu disposer d'une capacité à conduire des opérations militaires défensives et offensives dans le cyberespace en vue de garantir sa souveraineté nationale, dans le strict respect du droit national et international. Dans une démarche de transparence et de cohérence, elle a rendu ses doctrines accessibles au plus grand nombre en publiant plusieurs documents en 2019, notamment des éléments de doctrine militaire de lutte informatique offensive et le livre blanc sur l'application du droit international aux opérations militaires dans le cyberespace. Cette volonté de clarification et de partage de la vision de la France doit permettre de limiter les incompréhensions et les incertitudes, et ainsi contribuer à consolider la confiance et la transparence dans le cyberespace. La France encourage chaque État à procéder de même.

> Norme b : En cas d'incident informatique, les États devraient examiner toutes les informations utiles, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans cet environnement et la nature et l'ampleur des conséquences de l'incident.

La France a établi des procédures de gestion de crise ainsi que des structures et politiques nationales en cas d'incident lié aux technologies, notamment :

– Une cellule interministérielle de crise, déployée en cas de crise majeure ;

[3] Disponible à l'adresse suivante : www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

– Un centre de coordination de crise cyber composé de strates techniques ou opérationnelles et d'un niveau stratégique, interministériel et de haut niveau, qui se réunit tous les mois. En cas d'incident cyber, les participants du groupe de niveau stratégique analysent celui-ci dans un contexte plus large. Ils évaluent ses conséquences et peuvent envisager une attribution. La France considère que l'éventuelle attribution d'une attaque, ainsi que la décision de la rendre publique, est une prérogative souveraine.

La France a développé des moyens d'évaluer les incidents, notamment au travers d'une échelle de sévérité afin d'aider les décideurs à analyser et agir. Pour déterminer la sévérité d'un incident, la France prend par exemple en compte ses conséquences sur :

– Les intérêts de la nation, sa souveraineté, la démocratie

– La sécurité intérieure et civile

– La population et l'environnement

– L'économie

D'autres critères peuvent être pris en considération (l'intentionnalité, la dangerosité, l'attribution, le volume, la récurrence).

Norme c : Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications.

Afin de s'assurer que son territoire n'est pas utilisé afin de réaliser des actes malveillants, la France a :

– Imposé aux opérateurs d'infrastructures critiques nationales (loi n° 2013-1168) et aux opérateurs de services essentiels (loi n° 2018-133) le renforcement de la sécurité de leurs systèmes d'information et de communication – les « opérateurs d'importance vitale » ;

– Pénalisé (article 323-1 du Code pénal) les intrusions non autorisées dans les systèmes de sécurité de l'information des tiers ;

– Renforcé les capacités de l'Agence nationale de sécurité des systèmes d'information à détecter les incidents cyber qui toucheraient des opérateurs d'infrastructures critiques (loi n° 2018-607) ;

– Encouragé la divulgation responsable des vulnérabilités : les individus qui informent l'Agence nationale de sécurité des systèmes d'information de l'existence d'une vulnérabilité d'un produit ou service numérique sont protégés d'éventuelles poursuites judiciaires (loi n° 2016-1321).

Norme d : Les États devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'assister mutuellement, engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies de l'information et des communications et appliquer d'autres mesures collectives afin de parer à ces risques ; à cet égard, les États peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées.

Outre les éléments évoqués dans le volet coopération de notre réponse, la France a développé une palette de mesures afin d'améliorer la coopération avec ses partenaires pour prévenir l'utilisation criminelle et terroriste des technologies de l'information, notamment à travers son adhésion à la Convention sur la cybercriminalité (Convention de Budapest) et l'Appel de Christchurch visant à supprimer les contenus terroristes et extrémistes violents en ligne.

Sur le plan technique, l'Agence nationale de sécurité des systèmes d'information poursuit l'établissement de partenariats avec ses homologues de nombreux pays afin de favoriser le partage de données essentielles comme, par exemple, les informations concernant les vulnérabilités ou les failles de produits et services. Par ailleurs, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, établi au sein de l'Agence, est actif dans plusieurs réseaux multilatéraux (Forum of Incident Response and Security Teams, Task Force européenne de centres de réponse aux incidents de sécurité informatique, Groupe de centres gouvernementaux européens de réponse aux incidents de sécurité informatique, Réseau des centres de réponse aux incidents de sécurité informatique de l'Union européenne) grâce auxquels il entretient des contacts avec des centres de veille, d'alerte et de réponse aux attaques informatiques du monde entier.

> Norme e : Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression.

La France tient pour essentiel les principes suivant lesquels les droits de l'homme doivent être respectés et promus sur Internet et les individus doivent pouvoir bénéficier en ligne des mêmes droits que hors ligne. Au niveau national, la Commission nationale de l'informatique et des libertés est ainsi l'autorité compétente chargée depuis 1978 de garantir le respect des droits de l'homme et des libertés fondamentales, notamment le droit au respect de la vie privée et à la liberté d'expression.

La France s'est également investie en faveur de l'adoption d'une réglementation européenne prenant en compte les exigences de compétitivité et les potentialités du numérique tout en restant protectrice des citoyens et entreprises des États membres (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques, lutte contre les contenus terroristes en ligne). Cette volonté s'est illustrée lors de l'adoption du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information en 2016, ainsi que par le soutien à l'accroissement des compétences de l'Agence de l'Union européenne pour la cybersécurité. Enfin, la France œuvre pour que la politique industrielle de l'Union européenne soutienne les capacités de recherche et de développement de pointe afin de favoriser le déploiement de technologies et de services numériques de sécurité fiables et évalués indépendamment. La France a également participé activement à la rédaction des orientations de l'Union européenne portant sur la liberté d'expression, adoptées par le Conseil le 12 mai 2014, pour que la même liberté d'expression soit effective en ligne et hors ligne.

Au Conseil de l'Europe, la France soutient les actions en faveur de la protection des droits de l'homme sur Internet. La France a par exemple soutenu l'adoption du Guide des droits de l'homme pour les utilisateurs d'Internet, élaboré par le Comité des Ministres du Conseil de l'Europe en avril 2014, qui met notamment l'accent sur la liberté d'expression, l'accès à l'information, la liberté d'association, le droit à la vie privée, la protection des données personnelles et la protection contre les cybercrimes, qui doivent être les mêmes en ligne et hors ligne.

Aux Nations Unies, la France a soutenu l'adoption de toutes les résolutions du Conseil des droits de l'homme sur la promotion de la protection et la jouissance des droits de l'homme sur Internet ainsi que la résolution de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique.

Lors du Forum de Paris sur la Paix en novembre 2018, le Président Emmanuel Macron ainsi que 11 chefs d'États et de gouvernement ont également annoncé le lancement d'une initiative intergouvernementale sur l'information et la démocratie, en s'appuyant sur le travail déjà accompli sur le sujet par l'organisation non gouvernementale Reporters sans frontières. Cette initiative est aujourd'hui portée dans le cadre de l'Alliance pour le multilatéralisme lancée par la France et l'Allemagne.

> Norme f : Un État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public.

Dans l'esprit de cette norme, et comme évoqué plus haut, la France a pénalisé (article 323-1 du Code pénal) les intrusions non autorisées dans les systèmes de traitement automatisé de données de tiers.

Par ailleurs, la France a clairement établi dans ses éléments publics de doctrines, notamment dans son livre blanc publié en 2019 intitulé « Droit international appliqué aux opérations dans le cyberespace », la pleine application du droit international humanitaire aux opérations cyber menées en contexte de conflit armé et en lien avec ce conflit, comme cela sera évoqué plus en détail dans la section dédiée au droit international.

> Norme g : Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes.

Afin de contribuer au renforcement de la protection des infrastructures critiques, la France a développé, comme indiqué plus haut, un cadre réglementaire pour la protection des infrastructures critiques au travers d'obligations imposées aux opérateurs d'importance vitale de renforcer la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (loi n° 2013-1168 du 18 décembre 2013), ainsi qu'au travers du renforcement des compétences de l'Agence nationale de sécurité des systèmes d'information et de sa capacité à détecter des incidents. Les opérateurs d'importance vitale doivent en outre renforcer leurs mesures de sécurité et utiliser des systèmes de détection approuvés par l'Agence. La France encourage la coopération public-privé afin de développer la protection des infrastructures critiques en vue de définir un cadre efficace et adapté.

> Norme h : Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté.

Afin de mettre en œuvre cette norme, la France a, par exemple, développé un réseau de coopération de confiance à travers des partenariats techniques au niveau de

l'Agence nationale de sécurité des systèmes d'information qui permet entre autres des contacts entre centres de veille, d'alerte et de réponse aux attaques informatiques à travers des points de contact permanents.

Également, la France a mis en place pour l'organisation de la gestion des crises un mécanisme interministériel permanent d'analyse de la menace, de préparation et de coordination prenant la forme d'un centre de coordination des crises cyber. Ce dernier permet notamment un échange fluide d'information entre les différents services visant à améliorer la coordination nationale en vue de répondre à ces demandes.

La France a aussi mis une place un réseau de points de contact en lien avec la Convention de Budapest pour permettre le gel de données, qui est disponible 24 heures sur 24.

À l'OSCE, la France s'est engagée pour opérationnaliser la liste de points de contact (mesure de confiance 8, décision nº 1106 du Conseil permanent de l'OSCE) et accompagner divers travaux afin que chaque État établisse des canaux d'échange et d'information idoines (mesure de confiance 13, décision nº 1202 du Conseil permanent).

> Norme i : Les États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits informatiques, et devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes.

La France a encouragé le développement de normes et de standards pour l'industrie, notamment au travers de l'Appel de Paris. Elle a aussi promu le lancement de travaux internationaux sur le sujet dans différentes enceintes, principalement à travers l'équipe spéciale sur l'économie numérique au G20 et à l'OCDE.

La France a aussi promu l'utilisation de principes de certification par des tiers, sous l'autorité de l'Agence nationale de sécurité des systèmes d'information, afin de garantir le meilleur niveau de sécurité fourni par le marché. Ce processus est piloté au sein de l'Agence par le Centre de certification nationale. La France a également promu la mise en place de certifications de ce type au niveau de l'Union européenne.

En vue de renforcer la lutte contre la prolifération d'outils et techniques malveillants, la France a par ailleurs soutenu l'inscription des logiciels d'intrusion sur la liste des biens à double usage de l'Arrangement de Wassenaar.

> Norme j : Les États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent.

Comme indiqué plus haut, la France a adopté différentes mesures permettant le dévoilement responsable de vulnérabilités informatiques et développé des coopérations au niveau technique au travers de l'Agence nationale de sécurité des systèmes d'information, qui échange régulièrement avec ses homologues et partenaires sur les vulnérabilités et les solutions disponibles.

> Norme k : Les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État ; un État ne devrait pas se servir d'équipes

d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes.

La loi Godfrain (loi nº 88-19 du 5 janvier 1988) relative à la fraude informatique est la première loi française réprimant les actes de criminalité informatique et de piratage. Elle vient pénaliser le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données.

Le modèle de gouvernance français qui sépare les capacités offensives des capacités et missions défensives est une garantie du bon respect de ce principe. Les missions du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques sont notamment de coordonner et d'investiguer les réponses aux incidents cyber pour le Gouvernement français, mais aussi pour les opérateurs d'infrastructures critiques et de services essentiels tels que définis dans la loi, en les aidant à mettre en place le niveau de protection nécessaire, à détecter des vulnérabilités dans les réseaux et systèmes, à organiser la réponse aux incidents avec l'aide de partenaires si nécessaire et à participer à un réseau de confiance de centres de réponse aux incidents de sécurité informatique.

La reconnaissance de l'application du droit international, notamment de la Charte des Nations Unies au cyberespace, un autre principe agréé au sein du Groupe d'experts gouvernementaux

La France considère que l'émergence d'un cadre de cybersécurité collective ne pourra reposer que sur le respect des règles existantes du droit international. La France estime ainsi que la création d'un nouvel instrument international juridiquement contraignant spécifique aux enjeux de cybersécurité n'est pas nécessaire à ce stade. Dans le cyberespace comme dans les autres domaines, le droit international existant s'applique et doit être respecté.

Ainsi que le Groupe des experts gouvernementaux a pu le conclure dans son rapport publié en 2013, les principes et règles de droit international s'appliquent aux comportements des États dans le cyberespace. Si le cyberespace présente des spécificités propres (anonymat, rôle des acteurs privés), le droit international offre bien les moyens nécessaires pour encadrer de manière responsable le comportement des États dans cet environnement.

Le principe de souveraineté s'applique au cyberespace. À ce titre, la France réaffirme qu'elle exerce sa souveraineté sur les systèmes d'information, les personnes et les activités cyber sur son territoire ou relevant de sa juridiction, dans les limites de ses obligations découlant du droit international. La pénétration non autorisée de systèmes français qui entraînerait la production d'effets sur le territoire français par le biais de moyens cyber offensifs par une entité étatique ou des acteurs non étatiques agissant sous les instructions ou le contrôle d'un État pourrait constituer une violation de souveraineté.

Le champ des mesures que les États peuvent adopter pour réagir à une attaque informatique dont ils seraient victimes est fonction de la gravité des effets de celle-ci. Une opération cyber peut ainsi être considérée comme un recours à la force prohibé au titre de l'Article 2.4 de la Charte des Nations Unies. Le franchissement du seuil de l'emploi de la force n'est pas fonction du moyen cyber employé, mais des effets de l'opération cyber. Si ces derniers sont similaires à ceux qui résultent d'armes classiques, l'opération cyber peut être considérée comme un recours à la force. La France considère dès lors qu'une attaque informatique majeure perpétrée par un État ou des acteurs non étatiques agissant sous le contrôle ou les instructions d'un État, lorsqu'elle atteint par son ampleur ou ses effets un seuil de gravité suffisant (exemples : pertes humaines substantielles, dommages physiques considérables,

déficience des infrastructures critiques avec des conséquences significatives), peut constituer une « agression armée », au sens de l'Article 51 de la Charte des Nations Unies et justifier ainsi l'invocation de la légitime défense. Cette légitime défense peut être mise en œuvre par des moyens conventionnels ou cybernétiques, dans le respect des principes de nécessité et de proportionnalité. La caractérisation d'une attaque informatique en tant qu'« agression armée », au sens de l'Article 51 de la Charte, relève d'une décision politique prise au cas par cas à la lumière des critères établis par le droit international.

La France reconnaît par ailleurs la pleine applicabilité du droit international humanitaire aux opérations cyber conduites dans le cadre de conflits armés et en lien avec ceux-ci. À l'heure actuelle, les opérations de lutte informatique offensive sont combinées aux opérations militaires conventionnelles.

Malgré leur caractère dématérialisé, ces opérations restent soumises au champ d'application géographique du droit international humanitaire, c'est-à-dire que leurs effets sont limités au territoire des États parties en conflit armé international ou sur le territoire sur lequel se déroulent les hostilités dans le cadre d'un conflit armé non international. Les opérations de lutte informatique offensive mises en œuvre par les forces armées françaises sont soumises au respect des principes du droit international humanitaire dont :

– Le principe de distinction entre biens civils et objectifs militaires. À ce titre, les cyberattaques qui ne sont pas dirigées contre un objectif militaire déterminé ou qui sont mises en œuvre par des armes cyber qui ne peuvent pas être dirigées contre un objectif militaire déterminé sont prohibées. À cet égard, certaines données de contenu, bien que de nature intangible, peuvent constituer des biens civils protégés au titre du droit international humanitaire. Ce principe impose également de distinguer entre combattants ou membres de groupes armés organisés et personnes civiles. Les cyberattaques ne doivent pas non plus viser la population civile en tant que telle ni les personnes civiles, sauf si celles-ci participent directement aux hostilités et uniquement durant le temps de cette participation. En contexte de conflit armé, tout cybercombattant membre des forces armées d'une partie au conflit, tout membre d'un groupe armé organisé commettant des cyberattaques au détriment d'une partie adverse ou tout civil participant directement aux hostilités par le biais de moyens cyber peut faire l'objet d'une attaque par des moyens conventionnels ou cyber ;

– Les principes de proportionnalité et de précaution. Ces opérations doivent être conduites en veillant constamment à protéger les personnes et les biens civils des effets des hostilités. Les dommages collatéraux ne sauraient excéder l'avantage militaire direct et concret attendu. Le respect du principe de proportionnalité dans le cyberespace exige de prendre en compte l'ensemble des effets prévisibles de l'arme ainsi que leur caractère direct (dommages sur le système visé, interruption du service, etc.) ou indirect (effets sur l'infrastructure contrôlée par le système attaqué, mais également sur les personnes affectées par le dysfonctionnement ou la destruction des systèmes, ou par l'altération et la corruption de données de contenu), pour peu que ceux-ci entretiennent un lien de causalité suffisant avec l'attaque. Ce principe prohibe également le recours à des armes cyber qui ne peuvent être contrôlées dans le temps et l'espace.

Ces éléments sont notamment détaillés dans le rapport sur le droit international appliqué aux opérations dans le cyberespace, publié par le Ministère des armées le 9 septembre 2019 ainsi que dans les éléments publics de doctrine militaire française de lutte informatique offensive présentés la même année.

La France considère enfin comme essentiel de parvenir à une compréhension partagée, au niveau international, des obligations qui pèsent sur un État dont les infrastructures seraient utilisées à des fins malveillantes contre les intérêts d'un autre État. L'objectif est ici de clarifier l'application, dans le domaine cyber, du principe de diligence requise qui prévoit que tout État a l'obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »[4]. À ce titre, les États ne doivent pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide de moyens cybernétiques et doivent prendre toutes les mesures qui peuvent raisonnablement être attendues d'eux pour que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes. À ce titre, la France a identifié l'encadrement des possibilités de réponse à incident des acteurs privés comme un axe de travail important, qui pourrait concourir à la limitation d'actions ayant des effets négatifs sur les tiers, et donc au respect du principe de diligence requise[5]. Une meilleure compréhension de l'application de ce principe aux enjeux dans ce domaine permettrait de renforcer la coopération entre États en vue de protéger certaines infrastructures critiques, mais aussi de faire cesser des cyberattaques majeures qui transiteraient par le biais d'un État tiers.

Géorgie

[Original : anglais]
[29 mai 2020]

Alors qu'il cherche à promouvoir des services publics en ligne sûrs, résilients, sécurisés et fiables et à développer la société de l'information au sens large, le Gouvernement géorgien envisage attentivement toutes les possibilités d'appliquer les recommandations du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. La Géorgie entend contribuer activement aux principes et orientations formulés par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et prévoit de renforcer les mécanismes nationaux pertinents à cette fin.

Le présent document récapitule les principales nouveautés en matière de cybersécurité et de sécurité de l'information, ainsi que les efforts que fait la Géorgie au niveau national pour renforcer la sécurité de l'information et promouvoir la coopération internationale.

La Géorgie continue de chercher à renforcer sa position en matière de cybersécurité et entend se placer sur le devant de la scène internationale dans ce domaine. Étant donné les conditions géopolitiques dans lesquelles elle évolue, il ne fait pas de doute qu'elle a tout intérêt à améliorer sa cybersécurité. Le 28 octobre 2019, une cyberattaque de grande ampleur a été lancée contre les sites Web, les serveurs et d'autres systèmes informatiques de l'Administration de la Présidente, des tribunaux, de diverses assemblées municipales, d'organes de l'État, d'organisations du secteur privé et de médias. Elle visait à compromettre la sécurité nationale de la Géorgie et à nuire aux citoyens et aux institutions publiques du pays, en perturbant et en paralysant le fonctionnement de diverses organisations. L'enquête menée par les autorités géorgiennes ainsi que les informations recueillies grâce à la coopération de leurs partenaires ont permis de conclure que la cyberattaque avait été planifiée et exécutée par la Division principale de l'État-major général des Forces armées de la

[4] Affaire du Détroit de Corfou, Arrêt du 9 avril 1949 : *C.I.J. Recueil 1949*, p. 4.

[5] Cet encadrement – dont le principe devrait irriguer les travaux du Groupe d'experts gouvernementaux – devrait se faire sur la base d'une analyse de risques des mesures réalisables par les acteurs privés pour leur compte en réponse à un incident.

Fédération de Russie. L'attaque montre combien il importe que le Gouvernement poursuive l'action menée pour renforcer la cybersécurité du pays et indique, une fois de plus, qu'il est nécessaire de développer les partenariats internationaux dans le domaine de la cybersécurité.

La Géorgie alloue toutes ses ressources aux efforts visant à faire d'elle un pays plus fort, plus sûr et mieux protégé dans le cyberespace. Le Gouvernement entend en particulier donner les moyens à tous les groupes cibles de la société de l'information d'acquérir les connaissances et l'expérience nécessaires pour s'attaquer aux cybermenaces. Le modèle de gouvernance géorgien prévoit que les organisations publiques et privées puissent, ensemble et isolément, assurer la cybersécurité de manière durable en mettant en commun leurs ressources. En outre, la Géorgie a été reconnue comme un partenaire fiable dans le domaine de la cybersécurité par ses partenaires internationaux et jouit de leur soutien.

Le Gouvernement géorgien œuvre d'arrache-pied à fournir un cyberespace ouvert, sûr et sécurisé. La cybersécurité est un axe stratégique de la politique de sécurité nationale qu'il mène et fait l'objet d'une attention politique appuyée. À ce titre, le Gouvernement entend renforcer la cybersécurité et accroître la résilience du pays. Il considère qu'il découle de ses prérogatives de créer un environnement propice à la société de l'information, à l'économie numérique et à la gouvernance électronique au niveau national. Il a également endossé la responsabilité d'établir les cadres stratégiques, institutionnels, juridiques et réglementaires qui permettront d'assurer la sécurité et la sûreté des citoyens et des secteurs privé et public en ligne, en veillant à ce que l'environnement numérique soit utilisé de manière sûre.

Le renforcement de la coopération bilatérale, régionale et internationale dans le domaine de la cybersécurité est une priorité politique du Gouvernement. La Géorgie offre des exemples concluants de partenariats régionaux et internationaux ainsi que des exemples de partenariats dans le cadre d'instances multilatérales (Union européenne, Organisation du Traité de l'Atlantique Nord, Organisation pour la sécurité et la coopération en Europe, Organisation des Nations Unies, Partenariat oriental, Conseil de l'Europe, Agence de l'Union européenne pour la coopération des services répressifs, Organisation internationale de police criminelle, Agence de l'Union européenne pour la formation des services répressifs, Agence européenne chargée de la sécurité des réseaux et de l'information). Elle participe aussi activement aux projets et réunions consacrés à la cybersécurité.

Ces dernières années, les initiatives de coopération et de partenariat suivantes ont été prises :

- Ces dix dernières années, la Géorgie a adopté des mesures et engagé des réformes afin de renforcer la cybersécurité, ce qui a été favorablement accueilli sur la scène internationale. En ce qui concerne le renforcement de la cybersécurité, elle figure en bonne place au sein du Partenariat oriental. Elle est également un pôle régional de cybersécurité dans la région et organise des activités de renforcement des capacités et d'échange de bonnes pratiques et d'informations auxquelles participent divers pays de la région.

- La coopération entre la Géorgie et l'OTAN dans le domaine de la cybersécurité est en phase de développement. La Géorgie collabore étroitement avec les pays membres de l'OTAN et participe à titre individuel et collectif à différents projets organisés sous les auspices de l'organisation. Elle prend part notamment aux initiatives de formation stratégique et technique. Que ce soit au niveau du siège ou du Bureau de liaison, l'OTAN, aide les autorités numériques géorgiennes à mener des activités de sensibilisation et de formation qui s'adressent à différents groupes cibles dans le pays. La Géorgie fait régulièrement rapport de ses

réalisations en matière de cybersécurité et des initiatives menées en ce sens à la Commission OTAN-Géorgie et respecte scrupuleusement l'Engagement en faveur de la cyberdéfense de l'OTAN.

- Géorgie et Union européenne. Dans le cadre du projet quinquennal de l'« Union européenne pour la sécurité, la responsabilité et la lutte contre le crime en Géorgie » (EU4 Security, Accountability and Fight against Crime in Georgia), la Géorgie jouit de l'assistance de l'Union dans le domaine de la cybercriminalité, de la gestion des menaces informatiques et hybrides, de la gestion des frontières, de la protection civile et de la supervision du secteur de la sécurité. La Géorgie et l'Union européenne ont renforcé leur coopération dans le cadre de la Politique de sécurité et de défense commune, ce qui va dans le droit fil des objectifs fixés par l'Union à l'échelle internationale et permet de renforcer les capacités défensives géorgiennes et de contribuer à la sécurité nationale.

- Géorgie et OSCE. La Géorgie estime qu'il serait particulièrement utile de tisser un réseau fiable de pays partenaires qui s'appuierait sur des mesures de renforcement des capacités dans le domaine de la cybersécurité. Les points de contact de la Géorgie auprès de l'OSCE participent activement aux plateformes et initiatives organisées par l'organisation en matière de cybersécurité.

- Les Gouvernements géorgien et britannique ont signé un Mémorandum d'accord sur la coopération en matière de cybersécurité, dont le but est de renforcer le travail mutuel, de procéder à un échange de bonnes pratiques et de mieux harmoniser leurs approches respectives au sujet de divers aspects de la cybersécurité.

- Géorgie et pays du Partenariat oriental. L'Agence d'échange de données continue de coopérer avec les pays du Partenariat oriental dans le cadre de l'initiative EU4Digital visant à améliorer leur résilience informatique. Le projet CyberEast aide la Géorgie et les autres pays du Partenariat oriental à renforcer leurs capacités en matière de résilience informatique, de justice pénale et de preuves électroniques afin de lutter plus efficacement contre la cybercriminalité. L'accent est mis sur le renforcement des cadres juridique et politique, le renforcement des capacités des autorités judiciaires et des organes de détection et de répression, la coopération interinstitutions et l'application de mécanismes de coopération internationale efficaces dans le but de renforcer la confiance, y compris entre les prestataires de service et les services de détection et de répression, en matière de justice pénale, de cybercriminalité et de preuves électroniques.

- La Géorgie continue de renforcer la coopération régionale avec ses pays voisins dans le cadre de l'Organisation pour la démocratie et le développement. En 2019, les représentants de la Géorgie ont participé à diverses réunions de l'Organisation au siège de celle-ci, à Kiev.

- L'équipe d'intervention en cas d'atteinte à la sécurité informatique de Géorgie, un organe subsidiaire de l'Agence d'échange de données du Ministère de la justice, a signé un nombre considérable de mémorandums d'accord afin de partager ses connaissances et son expérience avec ses homologues des pays du Partenariat oriental (à savoir la Lituanie, la Roumanie, le Moldova, l'Ukraine et le Belarus). La Géorgie participe activement aux cyberexercices internationaux et analyse ses performances : elle se place systématiquement dans le haut du classement en matière de résultats observés.

Parallèlement aux connaissances colossales dont elle dispose dans ce domaine, la Géorgie tient compte de manière systématique des meilleures pratiques

internationales et de l'expérience pertinente, qui guident ses activités de coopération en faveur du renforcement de ses capacités stratégiques, juridiques et institutionnelles ainsi qu'en faveur de la transformation de la culture numérique.

En 2019, la troisième mouture de la stratégie nationale de cybersécurité et son plan d'action[6] ont été élaborés dans le cadre d'une étroite coopération entre les agences sectorielles de la cybersécurité[7]. Le Bureau du Conseil national de sécurité a coordonné ce processus. Parallèlement, les parties prenantes pertinentes du secteur privé, du monde universitaire et de la société civile ont également participé à divers processus. Alors que la Géorgie œuvre à l'élaboration d'un cadre national compatible avec les mécanismes de l'Union européenne et de l'OTAN, les processus de développement stratégique peuvent s'appuyer sur des consultations intensives avec des experts étrangers et des consultants nationaux intéressés. L'aide apportée par le Royaume-Uni aux acteurs géorgiens compétents en matière de cybersécurité dans le cadre de l'élaboration de la stratégie nationale de cybersécurité et de son plan d'action a une importance toute particulière. Ces documents seront entérinés par le Gouvernement géorgien en 2020. Ils feront également l'objet de la supervision de la Commission interinstitutions permanente, créée en janvier 2020 au Conseil national de sécurité et chargée de coordonner l'élaboration de documents conceptuels relatifs à la sécurité au niveau national. Le Conseil de sécurité national transmettra ensuite les projets de documents au Gouvernement pour approbation.

La Géorgie n'a de cesse de renforcer la mise en œuvre des cadres juridiques et réglementaires applicables au domaine informatique. Des cadres législatifs et réglementaires exhaustifs sur la cybersécurité ont été mis une place et des lois assurant la protection des droits des individus et organisations dans l'environnement numérique ont été adoptées. Ces lois portent sur la protection des infrastructures critiques, la responsabilité des fournisseurs d'accès à Internet, les obligations relatives à la communication d'incidents et la sécurité des transactions électroniques. À l'avenir, la Géorgie a l'ambition de mettre son cadre juridique relatif à la cybersécurité en conformité avec la Directive relative à la cybersécurité de l'Union européenne. Les organismes responsables ont en fait déjà entamé le processus de coopération avec l'Union européenne en 2019 et, d'ici la fin de l'année, la fiche de jumelage devrait être élaborée de sorte à aider la Géorgie dans ce processus d'harmonisation. Grâce au projet de jumelage, la Géorgie actualisera la loi sur la sécurité de l'information afin de définir clairement un cadre de gouvernance en matière de cybersécurité, de désigner les organismes responsables de la mise en œuvre de la Directive et de déterminer les rôles et responsabilités en matière de cybersécurité aux niveaux stratégique, opérationnel et tactique.

La Géorgie a également entamé un ambitieux processus d'élaboration et d'adoption de modèle de protection des infrastructures critiques conforme aux normes de l'Union européenne. En 2019, plusieurs ateliers ont été organisés afin de discuter d'un système permettant de déterminer quelles sont les infrastructures critiques et de coopérer dans le domaine du numérique. À cette fin, la Géorgie a élaboré une méthodologie et des questionnaires sur les infrastructures critiques et des acteurs du secteur privé représentant différents domaines et champs d'activités ont participé à ces travaux.

À l'heure actuelle, les prescriptions en matière de sécurité de l'information et de cybersécurité sont appliquées dans toutes les entités considérées comme faisant partie des infrastructures critiques. Les organismes publics compétents aident ces entités à mettre en œuvre les politiques de sécurité de l'information et de

[6] Prévus pour trois ans (2020-2023).

[7] Agence d'échange de données (Ministère de la justice), Bureau de la cybersécurité (Ministère de la défense), Agence opérationnelle et technique (Service de la sécurité d'État).

cybersécurité, formulent des recommandations et proposent leur expertise ainsi que des formations et d'autres activités, telles que des audits sur la sécurité de l'information, des tests de pénétration et d'autres services en matière de cybersécurité. Différents projets ont été lancés pour assurer la mise en place d'un système de gestion de la sécurité de l'information dans les entités considérées comme faisant partie des infrastructures critiques. Celles-ci reçoivent une assistance pour l'adoption de politiques relatives à la sécurité de l'information, la gestion des moyens et l'examen des politiques. Le Gouvernement fixe parallèlement des normes et procédures sur la sécurité de l'information au moyen de lois et de règlements (sur la base de la famille de normes ISO 27000) et propose des formations sur la sécurité informatique aux représentants de l'État et du secteur privé. Le prochain objectif de la Géorgie est d'élaborer et d'adopter des textes sur la protection des infrastructures critiques qui soient conformes à la Directive relative à la cybersécurité de l'Union européenne, en s'assurant que les dispositions juridiques élargies sur la sécurité des réseaux et des systèmes d'information soient applicables à la protection des infrastructures critiques.

Le Gouvernement géorgien tire parti, avec succès, de plateformes multipartites publiques-privées qui lui permettent de renforcer la confiance entre toutes les parties prenantes, de procéder à l'échange d'informations et de connaissances, d'élaborer de nouvelles initiatives et d'assurer la participation du secteur privé à l'élaboration de politiques et de stratégies. En 2019, l'Agence d'échange de données, qui est à la tête de ce processus de coopération publique-privée, a organisé myriade d'ateliers et de réunions avec les secteurs des finances, de l'énergie et des télécommunications afin de mettre en branle un processus de consultation visant à déterminer quelles sont les infrastructures critiques. Les parties prenantes privées participent à toutes les grandes consultations dans le cadre de projets horizontaux aux fins du renforcement des capacités stratégiques, politiques, juridiques et réglementaires.

La Géorgie mène des campagnes de sensibilisation systématiques et continues et organise des formations afin de promouvoir le professionnalisme dans le cyberespace et de renforcer les connaissances des groupes cibles. Une campagne de sensibilisation a eu lieu avec le concours des organismes publics géorgiens afin d'accroître les connaissances de la population en matière d'hygiène numérique. Des programmes de formation et de requalification en matière de cybersécurité sont également proposés à différents groupes cibles. Au fil des ans, les capacités de la Géorgie en matière de cybersécurité se sont développées grâce à différentes initiatives et à des programmes de formation. À cet égard, le Gouvernement a œuvré en faveur de l'amélioration des compétences des experts de la cybersécurité dans le secteur public et continue de le faire. Grâce à cette approche, ceux-ci disposent aujourd'hui de robustes qualifications professionnelles et nombre d'entre eux sont aujourd'hui en possession de certificats internationaux largement reconnus (SANS Institute, Association de l'audit et du contrôle des systèmes d'information, Organisation internationale de normalisation).

Enfin, la Géorgie continuera de participer activement au dialogue international sur la gouvernance d'Internet à d'autres initiatives concernant la cybersécurité collective.

Honduras

[Original : espagnol]
[17 avril 2020]

Rapport sur les mesures prises dans le domaine du cyberespace dans le contexte de la sécurité internationale

Dans le respect de la norme (ISO) 27001 de l'Organisation internationale de normalisation, qui porte sur la sécurité de l'information, et dans le but de créer une culture de travail en phase avec l'initiative de gouvernance numérique promue par la présidence de la République, la police nationale hondurienne a pris plusieurs mesures d'ordre interne concernant essentiellement les ressources Internet visées dans son manuel de sécurité de l'information, ledit document définissant clairement la stratégie de protection des activités opérationnelles de la police et réduisant ainsi la vulnérabilité des systèmes honduriens aux attaques ou actions malveillantes.

Ces mesures concernent notamment les points suivants :

1. Élaboration d'une politique de sécurité informatique

Des normes et lignes directrices régissant l'utilisation des outils technologiques sont élaborées pour protéger les ressources informatiques et matérielles dont l'institution a besoin pour exécuter son mandat constitutionnel et progresser ; dans un souci de bonne administration et de protection, le Honduras applique les meilleures pratiques et procède aux contrôles à même de garantir la confidentialité, la disponibilité et l'intégrité des informations en général.

2. Journées de formation

La Police nationale hondurienne, et plus particulièrement sa direction de la télématique, organise constamment des journées de sensibilisation aux enjeux du cyberespace à l'intention du personnel opérationnel et administratif, et participe à des activités de formation sur des questions telles que le harcèlement en ligne, l'ingénierie sociale, la désinformation, la cybercriminalité et la cybersécurité.

3. Mise en place d'un réseau local

L'intranet de la police, intitulé « Poliweb », permet au personnel de se tenir au courant des questions de cybercriminalité ; la police publie aussi des bulletins d'information essentiels sur l'actualité locale concernant la cybersécurité, dans lesquels sont également communiquées les politiques de sécurité informatique tirées du manuel pertinent.

En empruntant systématiquement ces voies de communication interne, réseau local ou intranet, la Police nationale minimise le risque que ses utilisateurs ne se rendent sur des sites inconnus, ce qui économise par ailleurs des ressources et de la bande passante.

4. Procédures de contrôle et d'enquête

L'équipe chargée de la sécurité de l'information assure une surveillance permanente du réseau de données institutionnel, recense les points vulnérables et relève les menaces introduites par le personnel lui-même sur ses ordinateurs, soit qu'il utilise l'Internet à mauvais escient soit qu'il ait cherché à circonvenir aux restrictions en place. Elle procède également aux enquêtes concernant les atteintes à la sécurité informatique du réseau institutionnel et à des contrôles à ce sujet. Les sections de gestion de l'information et de contrôle des incidents du département de la sécurité de

l'information analysent les failles qui pourraient compromettre les systèmes institutionnels et l'information qu'ils contiennent. Ces failles sont donc correctement prises en charges, la procédure officielle suivante étant prévue à cet effet :

- Inscription des données concernant l'éditeur du logiciel, la version, l'état de déploiement et le fonctionnaire responsable à l'inventaire des actifs informatiques ;
- Analyses bisannuelles de vulnérabilité ;
- Tenue à jour d'une liste de vulnérabilités ;
- Mise en place de délais de correction, des solutions étant prévues pour corriger les failles constatées ;
- Mise à l'essai des correctifs ou des patches de correction des failles avant leur déploiement en environnement de production.

5. Audits

L'exécution du plan d'audit annuel permet de vérifier l'application des politiques régissant l'utilisation du matériel informatique et de l'intranet institutionnel.

Les restrictions prévues concernent entre autres :

- L'interdiction d'installer des réseaux privés virtuels (VPN) sur les ordinateurs
- L'interdiction de différents navigateurs incognito tels que TOR, i2p, DUCK et WHONIX ;
- L'interdiction d'utiliser les réseaux sociaux (des exemptions étant prévues pour certaines adresses) ;
- L'interdiction de la navigation sur les sites de streaming à forte consommation tels que la télévision numérique ou autres sites de reproduction vidéo ;
- L'interdiction du stockage de la documentation personnelle et l'installation de logiciels sans rapport avec le travail.

L'historique des systèmes d'information, des serveurs, des dispositifs de réseau et autres services technologiques est conservé à des fins d'audit dans un registre rendant compte dans la mesure du possible des éléments suivants :

- Identifiant de l'utilisateur ;
- Date et heure de l'opération ;
- Adresse IP et nom du dispositif à partir duquel l'opération a été effectuée ;
- Type d'opération ;
- Identifiant de l'opération ;
- Données consultées, modifiées ou supprimées ;
- Tentatives de connexion infructueuses ;
- Reparamétrages du système ;
- Modification ou révocation des droits d'accès ;
- Fichiers consultés ;
- Alarmes déclenchées par des systèmes de contrôle ;
- Désactivation des mécanismes de protection.

6. Licence d'antivirus

La licence d'antivirus, qui est tenue à jour, constitue une couche de protection supplémentaire contre les logiciels malveillants. Le logiciel offre une protection contre le hameçonnage, les attaques de jour zéro et les rançongiciels et une mise à jour constante des correctifs de sécurité.

7. Gestion du pare-feu

La segmentation et l'activation des réseaux passe par un dispositif de pare-feu de protection périmétrique qui bloque les tentatives d'intrusion sur le réseau, comptabilise les connexions des utilisateurs internes et relève les sites Web consultés et les accès aux différents systèmes institutionnels.

8. Chiffrement des communications

En ce qui concerne la riposte aux atteintes à la sécurité nationale et leur prise en charge ainsi que la coordination interne de la Police nationale, un système de communication radio de pointe, doté d'une fonction de cryptage de sécurité, a été mis en place pour préserver l'intégrité des communications.

Ces mesures améliorent la protection des informations institutionnelles et contribuent aux efforts de prévention des cyberattaques face auxquelles nos systèmes seraient démunis en l'absence de mesures de protection. Il n'existe pas aujourd'hui de système absolument sûr, mais l'adoption de certaines mesures permet de minimiser les failles informatiques et de pourvoir à la gouvernance numérique du cyberespace et à la détection et la contention des cyberattaques.

Hongrie

[Original : anglais]
[15 mai 2020]

Questions relatives au cyberespace dans le contexte de la sécurité internationale

En décembre 2019, l'Assemblée générale a adopté la résolution intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », dans laquelle elle a invité les États Membres à continuer de communiquer au Secrétaire général leurs vues et leurs observations sur les efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine ainsi que sur la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

La Hongrie serait favorable à ce que le processus visant à délibérer de normes, règles et principes facultatifs de comportement responsable des États dans le cyberespace, de mesures de confiance et de droit international se poursuive de manière régulière sous les auspices de la Première Commission de l'ONU et au moyen de la création de Groupes d'experts gouvernementaux supplémentaires.

En 2018, la Hongrie a exprimé son soutien aux résolutions 73/266 et 73/27 de l'Assemblée générale, qui prévoyaient, en tant que mesure supplémentaire visant à s'attaquer aux menaces associées à l'utilisation des technologies numériques, la création d'un autre Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et d'un Groupe de travail à composition non limitée sur les progrès de

l'informatique et des télécommunications dans le contexte de la sécurité internationale, respectivement.

Bien qu'elle ait suivi avec grand intérêt le travail des Groupes d'experts gouvernementaux précédents, y compris dans le cadre de l'adoption de sa première Stratégie nationale de cybersécurité en 2013, la Hongrie a participé pour la première fois aux négociations à ce sujet. Lors des deux premières sessions officielles du Groupe de travail à composition non limitée, elle a été représentée consécutivement par son représentant permanent auprès de l'Organisation pour la coopération et la sécurité en Europe (OSCE), qui est également Président du Groupe de travail informel de l'OSCE sur la cybersécurité, et par le Coordinateur pour les questions numériques du Ministère des affaires étrangères et du commerce. Elle participe aussi activement aux consultations sur le projet de rapport du Président du Groupe de travail à composition non limitée. De manière générale, elle souscrit à la position de l'Union européenne.

La Hongrie est fortement favorable à un système multilatéral efficace qui repose sur un ordre international fondé sur des règles et qui permette de surmonter efficacement les difficultés qui se posent dans le cyberespace, témoin sa participation à différentes initiatives intergouvernementales et multipartites, ainsi que le soutien qu'elle a exprimé en faveur de celles-ci. La Hongrie réitère que le droit international existant est applicable à la conduite des États dans le cyberespace, comme indiqué dans les rapports consensuels du Groupe d'experts gouvernementaux de 2010, 2013 et 2015. Le non-respect des obligations découlant du droit international par des acteurs étatiques et non étatiques, tant dans le monde physique que dans le cyberespace, constitue toutefois une menace d'envergure pour la paix et à la sécurité internationales, ainsi que pour la souveraineté nationale de la Hongrie. Nous devons par conséquent être à même de dissuader et de prévenir les attaques classiques et non conventionnelles.

Soutien au Programme de désarmement

La Hongrie souscrit aux préoccupations exprimées par le Secrétaire général concernant l'utilisation accrue des technologies numériques à des fins malveillantes et, par conséquent, est favorable à la promotion d'un environnement numérique pacifique, qui constitue une priorité fondamentale du Programme de désarmement annoncé par le Secrétaire général en mai 2018. En signe de reconnaissance de l'engagement de haut niveau de la Hongrie, le Bureau des affaires de désarmement de l'ONU a déterminé que celle-ci était un partenaire pour la mise en œuvre de la 31e action du Programme, qui vise à instaurer un climat de responsabilité et à encourager le respect des nouvelles normes dans le cyberespace.

La Hongrie appuie les bons offices du Secrétaire général afin de prévenir l'escalade d'incidents informatiques et est favorable à l'opérationnalisation des normes facultatives de comportement dans le cyberespace et à la promotion de la collaboration en vue de réduire les écarts entre États Membres en matière de connaissances informatiques.

La cybersécurité en tant que question de sécurité nationale

En avril 2020, le Gouvernement a adopté la nouvelle Stratégie de sécurité nationale de la Hongrie [annexée à la Décision du Gouvernement 1163/2020 (IV.21.)] et, par conséquent, la Stratégie nationale de cybersécurité existante devra être modifiée. La nouvelle Stratégie de sécurité nationale donne un aperçu de l'évolution des menaces pour la sécurité depuis 2012. L'un des principaux objectifs de la Stratégie est de déceler les difficultés associées au développement rapide des technologies numériques, de s'y attaquer et d'y réagir.

Le nombre de cyberattaques et leur sophistication devraient aller croissant. Par conséquent, le Gouvernement hongrois fera tout ce qui est en son pouvoir, de concert avec d'autres parties prenantes, pour renforcer ses capacités et ainsi se prémunir contre des cyberattaques malveillantes contre ses infrastructures critiques et sensibiliser le public à l'hygiène numérique.

Surmonter les difficultés que posent la diffusion d'informations erronées et la désinformation en ligne et hors-ligne est une priorité absolue, en particulier aujourd'hui, alors que nous continuons de lutter contre la pandémie de maladie à coronavirus (COVID-19). En temps d'urgence nationale, les informations mensongères peuvent être particulièrement préjudiciables.

Le renforcement des cybercapacités offensives et défensives doit s'inscrire dans le cadre des obligations faites aux États par le droit international, sans quoi l'utilisation des technologies numériques à des fins offensives pourrait contribuer à la militarisation de l'espace numérique.

La Hongrie estime que les cybercapacités susceptibles de menacer la sécurité et la stabilité nationales constituent des armes, dont l'utilisation peut dépasser le seuil d'une attaque armée à laquelle les États peuvent également réagir par des moyens cinétiques dans le cadre de la légitime défense. Étant donné la difficulté d'identifier l'auteur de tels actes dans le cyberespace, les pouvoirs publics devraient faire preuve de la diligence requise en cas d'incident informatique et tenir compte de toutes les informations pertinentes, y compris le contexte dans lequel l'incident a lieu, sa nature et l'ampleur de ses répercussions.

Coopération internationale et initiatives multipartites

Membre de l'Union européenne, la Hongrie a participé activement à l'élaboration de la boîte à outils cyberdiplomatique qui doit permettre à l'Union de coordonner sa réaction face à des cyberactivités malveillantes commises de l'extérieur contre ses institutions ou ses États membres. Étant donné l'importance de la coopération internationale, elle est favorable à un dialogue renforcé avec ses partenaires stratégiques, ses alliés et d'autres organisations internationales.

Aucun pays ni aucune organisation n'est à même de combattre seul les menaces contemporaines pour la sécurité. Les partenariats, en particulier entre l'Union européenne et l'Organisation du Traité de l'Atlantique Nord, sont par conséquent plus importants que jamais. Il n'y a pas d'alternative à la poursuite et au renforcement de la coopération au cours des années à venir. Endiguer les menaces hybrides (y compris les menaces pour la cybersécurité) constitue indubitablement un aspect sur lequel les deux organisations devraient concentrer leurs efforts.

Les conflits dans le cyberespace devraient s'intensifier au cours des prochaines années et les écarts de capacités entre les pays technologiquement avancés et les pays en développement devraient être de plus en plus marqués. En juillet 2016, les alliés ont réaffirmé le mandat défensif de l'OTAN et reconnu que le cyberespace constituait un domaine opérationnel que l'OTAN se devait de défendre. En juillet 2018, ils ont une fois encore exprimé la volonté de l'OTAN de continuer de s'adapter aux cybermenaces en constante évolution, qui touchent à la fois les acteurs étatiques et non étatiques, y compris les acteurs parrainés par l'État. Les États membres de l'OTAN sont convenus d'intégrer les répercussions des cyberattaques, communiquées de manière volontaire par les alliés, à un cadre robuste de contrôle politique. Ayant réitéré le mandat défensif de l'OTAN, ses États membres se sont dits déterminés à avoir recours à toutes les capacités à leur disposition, y compris leurs cybercapacités, afin de dissuader toute cybermenace, de s'en prémunir et d'y réagir. L'OTAN s'engage à tisser de nouveaux partenariats avec l'industrie et les universités dans ses

pays membres afin de suivre le rythme des progrès technologiques grâce à l'innovation.

L'attachement de la Hongrie à la cybersécurité n'est pas neuf. Premier et seul traité international relatif à la lutte contre la cybercriminalité, la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest, a été entérinée dans la capitale hongroise en 2001 ; elle sert depuis lors d'orientation pour l'élaboration de lois nationales exhaustives sur la lutte contre la cybercriminalité et constitue un cadre international de coopération. La Hongrie a ratifié la Convention par le biais de la loi LXXIX de 2004. Non seulement la Hongrie est-elle partie à la Convention de Budapest, mais elle promeut également activement l'adhésion de pays tiers à cet instrument.

À titre de contribution nationale, le Représentant permanent de la Hongrie fait office, depuis 2017, de président du Groupe de travail informel de l'OSCE créé en vertu de la décision 1039 du Conseil permanent sur l'élaboration de mesures de confiance en vue de réduire les risques de conflit découlant de l'utilisation des technologies numériques. La Hongrie appuie les efforts visant à promouvoir une coopération plus étroite entre l'ONU et d'autres organisations régionales, telles que l'OSCE. Au niveau régional, nous soulignons l'importance de l'application des mesures de confiance adoptées par l'OSCE. Nous sommes également favorables à ce qu'une réflexion soit lancée au sein du Groupe de travail à composition non limitée sur la possibilité de porter les mesures de confiance régionales à l'échelle mondiale. Toutefois, la priorité devrait être d'opérationnaliser toutes les mesures de confiance régionales avec le même degré d'efficacité.

La Hongrie est l'un des rares pays à disposer de personnel consacré à la cyberdiplomatie. Le Coordinateur pour les questions numériques du Ministère des affaires étrangères et du commerce est responsable des activités de communication relatives au cyberespace dans le cadre de relations bilatérales et multilatérales, y compris avec l'Organisation des Nations Unies, l'Union européenne et l'OSCE, ainsi que dans le cadre d'initiatives multipartites, telles que le Forum mondial sur la cyberexpertise. La cyberdiplomatie est un domaine de coopération internationale relativement récent dont peut tirer parti le Gouvernement pour lutter contre les activités informatiques malveillantes.

La Hongrie contribue également aux efforts de renforcement des capacités dans les pays tiers. La cybersécurité fait partie intégrante de ces efforts et de la politique hongroise de coopération internationale pour le développement, en particulier vis-à-vis des pays d'Afrique partenaires. La Hongrie a, à ce titre, apporté une aide au développement dans le domaine de la sécurité des technologies numériques à l'Ouganda afin qu'il puisse relever les défis du XXI^{e} siècle. La Stratégie pour l'Afrique et la Stratégie de coopération internationale pour le développement pour la période 2020-2025, récemment adoptées par la Hongrie, consacrent d'ailleurs la cybersécurité comme un domaine fondamental de coopération.

En plus de participer à différentes négociations intergouvernementales, le Gouvernement hongrois est un fervent défenseur d'initiatives multipartites, telles que l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, qui donne suite à l'appel lancé pour une coopération plus approfondie aux fins de l'élaboration de normes, règles et principes de comportement des États dans le cyberespace. Des dizaines d'organisations hongroises du secteur privé se sont jointes aux efforts du Gouvernement à cet égard. La Hongrie appuie également l'Appel de Christchurch visant à supprimer les contenus terroristes et extrémistes violents en ligne, qui peuvent avoir des répercussions négatives sur les droits de la personne et sur la sécurité collective.

La Hongrie est également d'avis que les organisations non gouvernementales (société civile, milieux universitaires, secteur privé et communauté des technologies numériques) possèdent une vaste expertise technique ou les ressources nécessaires pour contribuer à la création d'un cyberespace sûr et durable dans le cadre de leur rôle et de leurs responsabilités. Les États, quant à eux, jouent un rôle de chef de file pour la promotion de la coordination et de la collaboration.

Indonésie

[Original : anglais]
[31 mai 2020]

Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale dans ce domaine

L'Indonésie compte plus de 170 millions d'utilisateurs d'Internet, ce qui représente 65 % de sa population. Les technologies numériques ont offert à l'Indonésie des possibilités essentielles pour la réalisation des objectifs de développement durable. Toutefois, les difficultés émanant du cyberespace se multiplient également. En 2019, l'Indonésie a subi plus de 220 millions de cyberattaques, ce qui entrave l'utilisation du cyberspace à des fins bénéfiques.

L'Indonésie envisage activement nombre de mesures visant à maximiser son potentiel numérique et lutter contre les menaces informatiques par le biais du renforcement de son cadre juridique, politique et institutionnel, ainsi que par le biais du renforcement des capacités et de la coopération internationale.

Efforts nationaux

L'Agence nationale de cybersécurité et de cryptographie a été créée en 2017 en tant qu'organisme centralisé responsable des questions relatives à la cybersécurité. L'équipe nationale d'intervention en cas d'atteinte à la sécurité informatique a été mise sur pied au sein de l'Agence afin de pouvoir rapidement réagir aux cyberattaques prenant pour cible les infrastructures de l'État ou du secteur privé. Une équipe d'intervention en cas d'atteinte à la sécurité informatique a également été formée au sein de chaque agence gouvernementale centrale ainsi qu'au niveau des districts afin de lutter contre les incidents informatiques et de restaurer les systèmes touchés dans les 34 provinces indonésiennes.

Afin de renforcer le cadre juridique et politique national, l'Indonésie a promulgué la loi sur l'information et les transactions électroniques ainsi que la Feuille de route nationale sur le commerce électronique pour la période 2017-2019. Cette dernière prévoit des mesures visant à assurer la sécurité des transactions électroniques et numériques. L'Indonésie a également adopté les Orientations de cyberdéfense en vertu du Règlement nº 82 de 2014 du Ministère de la défense. Le système indonésien de normalisation a aussi adopté les normes internationales pour la sécurité des technologies numériques, à savoir les normes ISO/CEI 27001 et ISO 15408.

Le projet de loi sur la cybersécurité de 2020 a été placé au premier rang des priorités et le processus législatif se poursuit. L'Indonésie est également en train d'élaborer une stratégie nationale de cybersécurité pour la période 2020-2024, qui repose sur cinq piliers : résilience informatique, renforcement du cadre juridique, capacités liées aux technologies numériques, appui à la croissance économique numérique et coopération nationale et internationale.

L'Indonésie est également déterminée à renforcer la coopération au niveau national, en particulier avec les entreprises publiques, le secteur privé et l'industrie,

afin de favoriser l'instauration d'une culture inclusive de la cybersécurité. En 2018, le Gouvernement a lancé la campagne de développement des connaissances en matière de cybersécurité, qui vise à promouvoir un accès sécurisé à Internet, la déontologie sur les médias sociaux et une utilisation responsable d'Internet et à donner aux parents des orientations leur permettant d'assurer la sécurité de leurs enfants sur Internet, et qui vise à lutter contre les canulars et le harcèlement en ligne.

Efforts internationaux

L'Indonésie n'a de cesse de promouvoir, par le biais de multiples initiatives, la coopération mutuelle, les bonnes pratiques et les capacités nécessaires en vue d'aboutir à un instrument efficace en matière de cybersécurité qui pourrait être, à terme, universellement adopté.

En ce qui concerne les efforts qu'elle fait au niveau mondial et multilatéral, l'Indonésie participe activement aux travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, y compris en sa qualité de coordinatrice du Groupe de travail sur le désarmement du Mouvement des pays non alignés. Elle fait également partie à l'heure actuelle des 25 membres du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

À l'échelle régionale, l'Indonésie a contribué à l'élaboration de mesures de confiance dans le cadre de l'Association des nations de l'Asie du Sud-Est (ASEAN), en appuyant entre autres la création de points de contact au sein des organismes sectoriels compétents de l'Association pour les questions informatiques conformément aux piliers de l'ASEAN sur la sécurité politique et sur la communauté économique. Elle y a également contribué par le biais d'un échange d'information, d'une collaboration régulière en matière de cybersécurité et de dialogues entre États membres. Ceux-ci ont également renforcé la coopération dans le domaine de la cybersécurité en créant un comité de coordination intersectoriel. Grâce au Forum régional de l'ASEAN, les délibérations relatives aux mesures de confiance dans le contexte de la cybersécurité ne se limitent plus aux pays de la région et font intervenir d'autres pays et partenaires.

En outre, l'Indonésie entretient un dialogue et des liens de coopération avec divers États et partenaires. Elle continuera de contribuer de manière significative aux efforts visant à favoriser un comportement responsable des États et à promouvoir un environnement numérique ouvert, sûr, stable, accessible et pacifique.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

L'utilisation abusive du cyberespace par des acteurs étatiques et non étatiques, y compris des intermédiaires, présente des risques pour la paix et la sécurité internationales ainsi que pour la stabilité politique, économique et sociale nationales. Les pays du monde entier se tournent vers les technologies numériques pour lutter contre les répercussions multidimensionnelles de la pandémie de maladie à coronavirus (COVID-19). Des acteurs numériques mal intentionnés pourraient tenter de s'attaquer aux systèmes informatiques et à la diffusion d'informations dans le cyberespace, en particulier.

La compréhension mutuelle, la coopération, la collaboration, les mesures de confiance et de renforcement des capacités et l'assistance sont essentielles pour renforcer la sécurité et la stabilité dans le cyberespace. Les efforts bilatéraux,

régionaux et mondiaux en ce sens doivent être appuyés et perçus comme complémentaires, plutôt que comme entrant en concurrence.

L'Indonésie est favorable à la poursuite du dialogue et à l'application des normes non contraignantes énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux. Elle redit que l'Organisation des Nations Unies et les organisations régionales jouent un rôle fondamental dans la promotion des discussions et la mise en œuvre des 11 normes et des mesures de confiance et de renforcement des capacités en matière de cybersécurité, en particulier en vue de réduire la fracture numérique entre les pays.

L'Indonésie est d'avis que des normes facultatives et non contraignantes constituent un cadre important pour le comportement responsable des États. Alors qu'il convient de combler les lacunes relatives à la gouvernance du cyberespace, elle est favorable au développement de la pratique des États et de la pratique coutumière.

L'Indonésie est prête à discuter de l'application du droit international existant dans le cyberespace, y compris l'opportunité d'une *lex specialis*. Elle souligne que le cyberespace devrait être utilisé en conformité avec les principes du droit international, en particulier la souveraineté, la non-ingérence et le règlement pacifique des différends, ainsi que les droits de l'homme et la Charte des Nations Unies.

L'Indonésie serait favorable à ce que soit élaborée une déclaration conformément à laquelle tous les États s'abstiendraient de militariser le cyberespace, puisque la militarisation de l'espace numérique porte préjudice à la paix et la sécurité internationales et est contraire aux obligations découlant du droit international.

L'Indonésie souligne l'importance de renforcer la compréhension mutuelle et la mobilisation, en particulier parmi les pays et régions qui n'ont pas participé de manière adéquate aux délibérations et à l'élaboration de mesures en matière de cybersécurité.

Irlande

[Original : anglais]
[30 mai 2020]

L'Irlande se félicite de la possibilité qui lui est donnée de répondre à la demande formulée par le Secrétaire général en application du paragraphe 2 de la résolution 74/28, intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ». Elle souscrit également aux observations de l'Union européenne.

Les technologies numériques sont bénéfiques pour la société et les États ; elles facilitent la communication, l'éducation, l'innovation et l'activité économique et favorisent la prospérité. Toutefois, dans un monde de plus en plus connecté, l'utilisation abusive de ces technologies peut également avoir des conséquences éminemment négatives, et l'augmentation du nombre d'activités informatiques à des fins malveillantes, y compris pendant la présente pandémie, est une source de préoccupation majeure pour l'Irlande. Ces activités nuisent aux citoyens et sapent leur confiance vis-à-vis des institutions. Leurs répercussions se font également sentir au niveau de la société et des États, où elles peuvent entraîner des conflits ou les aggraver.

L'Organisation des Nations Unies demeure l'instance idoine pour s'attaquer aux difficultés liées à l'utilisation abusive des technologies numériques et aux activités informatiques malveillantes, qui ont des répercussions sur les trois piliers de son action : la paix et la sécurité, les droits de la personne et le développement durable.

En tant qu'économie comptant un important secteur des technologies numériques et en tant que pays profondément attaché à l'ONU, l'Irlande continuera d'appuyer les efforts que l'Organisation fait pour promouvoir et favoriser le comportement responsable des États dans le cyberespace. Elle continuera d'œuvrer de manière volontariste et dans un esprit de collaboration avec ses partenaires à l'ONU et sur la scène internationale afin d'appuyer la création d'un cyberespace ouvert, libre, sûr et sécurisé, de promouvoir la liberté d'association, d'expression et de réunion en ligne, d'atténuer les risques de conflit, de promouvoir la paix et de s'assurer que les avantages socioéconomiques qu'offre le cyberespace sont accessibles par tous, y compris en vue d'appuyer la réalisation des objectifs de développement durable. L'Irlande estime que ce n'est que par le biais d'un travail multilatéral impliquant diverses parties prenantes qu'il sera possible de pérenniser les progrès faits pour surmonter les difficultés. Elle est attachée à cette démarche et a, à ce titre, mis en œuvre différentes initiatives. Elle a notamment créé en 2019 le groupe Cyber Irlande, qui a été financé par des fonds publics et rassemble divers acteurs de l'industrie, du monde universitaire et des pouvoirs publics afin de procéder à un dialogue et de promouvoir la coopération, de sensibiliser le public aux questions informatiques et aux possibilités d'emploi dans ce domaine, et de favoriser l'innovation dans le secteur de la cybersécurité en Irlande. L'approche de l'Irlande sur la scène internationale s'ancre également dans cet engagement. À ce titre, nous saluons les initiatives menées à l'ONU et au sein d'autres instances visant à promouvoir une coopération et un dialogue plus larges, y compris par le biais du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. L'Irlande soutient également le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

En ce qui concerne les questions relatives à la cybersécurité, l'approche de l'Irlande se fonde sur son engagement en faveur de l'applicabilité et de la centralité du droit international, y compris la Charte des Nations Unies, le droit international humanitaire et le droit international des droits de l'homme. L'Irlande salue également le consensus trouvé par l'Assemblée générale en 2015 quant au fait que l'utilisation des technologies numériques par les États devrait être guidée par le rapport de 2015 du Groupe d'experts gouvernementaux, qui énonce 11 normes facultatives et non contraignantes de comportement responsable des États. Associées au droit international et complétées par des mesures de renforcement des capacités visant à favoriser la résilience et à faciliter l'accès aux technologies numériques ainsi que par des mesures de confiance appelées à atténuer les risques de conflits armés, ces normes constituent selon l'Irlande un cadre robuste permettant de favoriser le comportement positif des États dans le cyberespace. Les initiatives de renforcement des capacités dans le domaine des technologies numériques contribuent également à réduire la fracture numérique mondiale, à transformer la vie de la population et des communautés, à favoriser la prospérité et à atteindre les objectifs de développement durable, y compris eu égard aux questions de genre.

Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

Stratégie nationale de cybersécurité pour la période 2019-2024

Dans un cyberespace interconnecté, tous les États doivent veiller à renforcer leur résilience face aux risques informatiques, tant à l'échelle nationale qu'internationale. La Stratégie nationale de cybersécurité pour la période 2019-2024[8] de l'Irlande énonce des mesures et objectifs fondamentaux à cet égard. Du fait qu'elle

[8] Disponible à l'adresse suivante : www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

entend protéger l'Irlande, sa population et ses infrastructures critiques contre les menaces pour la cybersécurité, la Stratégie contribue à l'objectif des Nations Unies de promouvoir le comportement responsable des États dans le cyberespace et de pérenniser la paix et la sécurité internationales. Elle est également le socle sur lequel repose l'engagement international de l'Irlande en faveur d'un cyberespace libre, ouvert, pacifique et sûr. La politique de cybersécurité de l'Irlande est exécutée par le Centre national de cybersécurité, qui contribue aux travaux des Nations Unies en promouvant le dialogue sur les questions relatives à la cybersécurité, en renforçant la confiance et la sécurité dans le cyberespace et en collaborant avec des organismes partenaires et d'autres parties prenantes sur la scène internationale.

Les principaux objectifs de la Stratégie de cybersécurité de l'Irlande sont les suivants :

- Continuer de renforcer sa capacité à déceler et gérer les atteintes à la cybersécurité et y réagir ;
- Définir et protéger les infrastructures critiques en renforçant la résilience face aux cyberattaques ;
- Accroître la résilience et la sécurité des systèmes informatiques du secteur public afin de mieux protéger les services dont dépendent les citoyens et de protéger leurs données ;
- Investir dans des initiatives éducatives visant à former la main d'œuvre aux technologies informatiques de pointe et à des carrières dans le domaine de la cybersécurité ;
- Sensibiliser les entreprises à leur responsabilité de sécuriser leurs réseaux, leurs dispositifs et leurs informations et promouvoir la recherche-développement en matière de cybersécurité en Irlande, y compris en facilitant les investissements dans les nouvelles technologies ;
- Continuer à œuvrer avec les partenaires internationaux et les organisations internationales afin que le cyberespace demeure ouvert, sûr, unitaire et libre et qu'il puisse contribuer au développement socioéconomique et à un renforcement durable des capacités ;
- Accroître de manière générale le niveau de compétences et de connaissances des individus en ce qui concerne l'hygiène numérique de base et les y aider au moyen d'informations et de formations.

Livre blanc sur la défense

Le Livre blanc sur la défense de l'Irlande (publié en 2015[9] et mis à jour en 2019[10]) fait état des dangers associés aux activités informatiques malveillantes à l'échelle nationale et internationale, y compris pour les infrastructures critiques et les services essentiels. Il y est également indiqué que les systèmes informatiques peuvent être utilisés de manière abusive afin de porter atteinte aux valeurs fondamentales, y compris la dignité humaine, la liberté et la démocratie. Le Livre blanc sur la défense et la Stratégie nationale de cybersécurité continuent de sous-tendre l'engagement de l'Irlande en matière de technologies numériques et pour les questions connexes.

[9] Disponible à l'adresse suivante : https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf.

[10] Disponible à l'adresse suivante : www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/.

Approche au niveau bilatéral, régional et multilatéral

L'Irlande continue de promouvoir le dialogue sur les technologies numériques et les questions informatiques dans le cadre des relations bilatérales qu'elle entretient avec d'autres États, ainsi qu'au sein d'instances régionales et multilatérales.

Elle salue l'Organisation pour la coopération et la sécurité en Europe (OSCE) et d'autres organisations régionales du monde entier pour les efforts qu'elles font pour promouvoir des mesures de confiance et de renforcement des capacités.

L'Irlande est favorable aux initiatives visant à promouvoir la confiance, la sécurité et la paix dans le cyberespace menées par des États et d'autres acteurs, y compris l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Elle souscrit également à l'Appel de Christchurch visant à supprimer les contenus terroristes et extrémistes violents en ligne. Elle est membre de la Coalition pour la liberté en ligne, composée de 31 États qui œuvrent de concert à promouvoir la liberté sur Internet.

L'Irlande a également envoyé au Centre d'excellence pour la cyberdéfense en coopération, basé à Tallinn, une lettre d'intention qui exprimait son intérêt de rejoindre le Centre afin de pouvoir contribuer, dans un esprit de collaboration avec les États animés du même esprit, à la lutte contre les menaces pour la cybersécurité. N'étant pas membre de l'OTAN, elle adhérera au Centre comme Participant contribuant.

Promouvoir la coopération internationale dans l'Union européenne

En tant qu'acteur volontariste, l'Irlande continue de jouer pleinement son rôle au sein de l'Union européenne dans le domaine de la cybersécurité et coopère étroitement avec ses partenaires de l'Union afin de promouvoir un cyberespace mondial ouvert, libre, stable et sûr, ce qui contribue à la prévention des conflits, y compris grâce aux initiatives de cyberdiplomatie et à la boîte à outils de l'Union. L'Irlande participe également à diverses initiatives de l'Agence européenne de défense dans le cadre du développement de ses propres capacités.

Promouvoir la coopération internationale à l'Organisation des Nations Unies

Au niveau de l'ONU, l'Irlande appuie les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (voir ci-dessous) et contribue activement aux séances du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Le 22 mai 2020, l'Ambassadeur de l'Irlande auprès de l'Organisation a également pris la parole à une réunion du Conseil de sécurité organisée selon la formule Arria sur la stabilité informatique, la prévention des conflits et le renforcement des capacités. Il a alors mis en exergue l'engagement de l'Irlande à œuvrer avec les Nations Unies dans le cadre de multiples activités dans ce domaine, y compris dans le cadre d'activités visant à tirer parti des technologies numériques et du cyberespace pour atteindre les objectifs de développement durable, en particulier l'objectif relatif à l'égalité entre les sexes.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Principes généraux

En ce qui concerne la promotion de la cybersécurité, l'Irlande est favorable à une approche multilatérale, qui soit technologiquement neutre et qui s'appuie sur un

ordre international fondé sur des règles. Elle estime que la participation de parties prenantes (y compris la société civile, les universités et les représentants de l'industrie et des milieux techniques) et leurs contributions aux récentes réunions du Groupe de travail à composition non limitée ont enrichi les débats. Ces parties prenantes joueront un rôle de plus en plus fondamental en conseillant les États sur l'évolution du secteur des technologies numériques et en contribuant directement à un cyberespace sûr et stable. L'Irlande considère que favoriser la participation des parties prenantes aux réunions et débats futurs est désirable et nécessaire et qu'il faudrait l'officialiser.

Menaces existantes et émergentes

La Stratégie nationale de cybersécurité de l'Irlande prend en compte les retombées grandissantes et positives des technologies numériques sur le développement socioéconomique. Toutefois, elle met également en exergue la recrudescence de la cybercriminalité, du vol de propriété intellectuelle, de la diffusion d'informations mensongères et de l'utilisation par les États de cybercapacités offensives. La pandémie de maladie à coronavirus (COVID-19) a montré à quel point nous dépendons des technologies numériques pour travailler et communiquer avec souplesse et en toute sécurité, ainsi que pour poursuivre l'activité économique. Cependant, elle a également mis en lumière les agissements d'acteurs mal intentionnés qui exploitent les vulnérabilités existantes, qu'elles soient humaines ou techniques, afin de commettre des crimes en ligne, de diffuser des informations mensongères et de semer la confusion, de susciter la méfiance et de diviser. L'Irlande prend note avec préoccupation des récentes attaques informatiques prenant pour cible les services médico-sanitaires et les services connexes. Ces attaques contre des services de santé et d'autres services essentiels mettent en danger des vies. À l'instar de ses partenaires de l'Union européenne, l'Irlande a condamné ces attaques et encouragé les États à faire preuve de la diligence requise et à prendre les mesures qui s'imposent contre les auteurs de telles activités sur leur territoire, conformément au droit international et aux rapports du Groupe d'experts gouvernementaux adoptés par consensus en 2010, 2013 et 2015.

Droit international

L'Irlande est fermement convaincue de l'applicabilité et de la centralité du droit international, y compris la Charte des Nations Unies, le droit international humanitaire et le droit international des droits de l'homme, dans le cyberespace. Les droits de la personne et les libertés fondamentales doivent être respectés aussi bien en ligne que hors ligne. Étant donné qu'il existe déjà un cadre juridique international, l'Irlande a exprimé ses réserves quant aux appels lancés pour l'élaboration d'un nouvel instrument juridique, y compris lors des récentes réunions du Groupe de travail à composition non limitée. Elle se félicite toutefois du dialogue en cours visant à promouvoir plus avant une interprétation commune de l'application du droit international existant à l'utilisation des technologies numériques par les États.

Normes, règles et principes de comportement responsable des États

L'Irlande est favorable aux normes, règles et principes facultatifs et non contraignants de comportement responsable des États énoncés dans le rapport de 2015 du Groupe d'experts gouvernementaux. Elle se félicite du consensus trouvé à l'Assemblée générale selon lequel les États devraient être guidés par ledit rapport lorsqu'ils ont recours aux technologies numériques. Ces normes favorisent la stabilité et la sécurité de l'environnement numérique mondial et peuvent contribuer au maintien de la paix internationale. La Stratégie nationale de cybersécurité et les politiques de l'Irlande s'inspirent de ces normes, règles et principes, y compris eu égard au renforcement durable des capacités. À l'ONU, l'Irlande a lancé un appel à

élaborer des orientations quant à la manière dont les normes existantes, qui ont été entérinées par tous les États Membres par consensus, peuvent être appliquées et mises en pratique.

Mesures de renforcement des capacités

La Stratégie nationale de cybersécurité de l'Irlande prévoit un engagement en faveur de mesures de renforcement durable des capacités. En ce qui concerne le renforcement de la résilience des États face aux activités informatiques malveillantes, l'atténuation des vulnérabilités, la protection des infrastructures critiques et la promotion de l'accès de tous les États aux avantages découlant de l'utilisation des technologies numériques, l'Irlande est également attachée à une approche multilatérale et multipartite. Elle est également d'avis qu'il est essentiel que les États et les principales parties prenantes aient la possibilité de participer aux discussions mondiales en matière de cybersécurité. À cet égard, elle se félicite d'avoir parrainé la réunion intersessions informelle du Groupe de travail à composition non limitée, qui a eu lieu du 2 au 4 décembre 2019 et a rassemblé les États et les parties prenantes, y compris des représentants d'organisations non gouvernementales et de la société civile, des experts techniques, des chercheurs, des universitaires et des acteurs du secteur privé. L'Irlande a également appuyé les efforts visant à réduire la fracture numérique entre femmes et hommes. Elle serait favorable à ce qu'un lien plus étroit soit établi entre les initiatives et débats relatifs au renforcement des capacités à l'ONU, les objectifs de développement durable et le programme pour les femmes et la paix et la sécurité.

Italie

[Original : anglais]
[29 mai 2020]

Introduction

L'Italie souscrit aux observations et à la contribution au présent rapport soumises par l'Union européenne et souhaiterait transmettre les informations nationales suivantes au Secrétaire général.

Aux fins du présent rapport, l'Italie n'aura pas recours à l'expression « sécurité de l'information », qui n'est pas en usage dans l'ordre juridique italien. D'autres termes, tels que « cybersécurité » ou « sécurité des réseaux et des systèmes d'information », sont quant à eux usités et donc préférables. La liberté d'expression, que ce soit en ligne ou hors ligne, est consacrée par la Constitution italienne et par l'article 19 du Pacte international relatif aux droits civils et politiques, que l'Italie a ratifié en 1978.

En vertu du décret du Premier Ministre italien du 17 février 2017, qui énonce des orientations pour la protection du cyberespace et la sécurité des technologies numériques, le terme « cybersécurité » fait référence à la protection du cyberespace par le recours à des mesures de sécurité physique et logistique et à des procédures appropriées dont le but est de prévenir et de circonscrire les atteintes à la sécurité, qu'elles soient intentionnelles ou accidentelles, impliquant l'acquisition et le transfert abusifs, la modification ou la destruction illégitime de données, ou encore la prise de contrôle injustifiée, l'endommagement, la destruction ou l'interruption du fonctionnement des réseaux et des systèmes informatiques, ou de leurs composantes.

De même, conformément au décret législatif 65/2018, qui traduit dans le droit italien la Directive de l'Union européenne sur la sécurité des réseaux et systèmes d'information, l'expression « sécurité des réseaux et systèmes d'information » fait

allusion à la capacité d'un réseau ou d'un système informatique à résister, dans un certain degré de confidentialité, à tout acte visant à porter atteinte à la disponibilité, à l'authenticité, à l'intégrité ou à la confidentialité de données stockées, transmises ou traitées et des services disponibles ou accessibles au moyen dudit réseau ou dudit système informatique.

Efforts faits au niveau national pour renforcer la cybersécurité : cadre institutionnel et normatif

En décembre 2013, l'Italie a adopté le Cadre stratégique national pour la sécurité du cyberespace, qui fait état des menaces grandissantes et en constante évolution associées à l'utilisation des technologies numériques et dont l'objectif est de renforcer les capacités et la résilience informatiques du pays. Les plans d'action connexes, dont le dernier a été publié en mars 2017 et adopté en vertu du décret du Premier Ministre du 17 février 2017 susmentionné, définissent un certain nombre d'actions, de mesures et de priorités afin de mettre en œuvre le Cadre stratégique.

Le décret détermine l'architecture nationale de cybersécurité et ses mécanismes de gouvernance. Il prévoit également la création au Département du renseignement et de la sécurité d'une Cellule de cybersécurité, qui est chargée de prévenir les crises informatiques nationales, de s'y préparer et de coordonner dans les secteurs privé et public la réponse apportée et le rétablissement après une crise, conformément aux décisions du Premier Ministre.

La Cellule de cybersécurité est constituée d'un secrétariat et d'un conseil conjoint présidé par le Directeur général adjoint aux affaires informatiques du Département du renseignement et de la sécurité et rassemble des représentants de la communauté du renseignement (Département du renseignement et de la sécurité, Agence externe de renseignement et de sécurité et Agence interne d'information et de sécurité), le Conseiller militaire du Premier Ministre, les Ministères des affaires étrangères et de la coopération internationale, de l'intérieur, de la justice, de la défense, de l'économie et des finances, et du développement économique, ainsi que l'Agence pour une Italie numérique. Un représentant du Bureau central du Département du renseignement et de la sécurité participe également aux réunions lorsqu'il y est question d'incidents compromettant des systèmes informatiques classifiés.

En cas de crise informatique nationale, la Cellule peut également faire intervenir des représentants du Ministère de la santé, du Ministère de l'infrastructure et des transports, et des sapeurs-pompiers. Sur la base des informations qu'elle transmet, le Premier Ministre peut déclarer l'état de crise informatique lorsqu'une atteinte à la sécurité informatique ne peut être circonscrite par l'entité compétente et requiert, en raison de sa portée, de son intensité ou de sa nature, une réponse conjointe, dont la Cellule de cybersécurité assure la coordination.

Outre le décret du Premier Ministre, les lois suivantes ont été adoptées :

- Le décret législatif 65/2018, qui traduit dans le droit italien la Directive de l'Union européenne sur la sécurité des réseaux et des systèmes d'information et désigne le Département du renseignement et de la sécurité comme point de contact unique pour la sécurité des réseaux et des systèmes d'information ;
- Le périmètre national de cybersécurité (loi 133/2019), entré en vigueur en novembre 2019, s'applique aux organismes privés et publics exerçant des fonctions essentielles ou fournissant des services cruciaux pour la réalisation des activités considérées vitales du point de vue des intérêts nationaux italiens. Les organismes publics et privés concernés sont inclus dans le « périmètre » en fonction d'une échelle de priorités relatives à la sécurité nationale. La loi porte

sur les réseaux, les systèmes informatiques et les services appartenant aux organismes précédemment mentionnés ou exploités par ceux-ci et ayant une importance particulière pour la sécurité nationale. Elle prévoit ce qui suit :

– Des notifications en cas d'incident, afin de garantir que les entités responsables de la prévention et de la gestion des atteintes à la sécurité informatique ainsi que de la préparation à celles-ci, à savoir la Cellule nationale de cybersécurité et l'Équipe d'intervention en cas d'atteinte à la sécurité informatique, qui dépendent toutes deux du Département du renseignement et de la sécurité, puissent avoir accès en temps réel aux informations nécessaires ;

– Des mesures de sécurité portant sur des questions, procédures et processus institutionnels, y compris les achats de technologies numériques ;

– Un contrôle technologique des produits et services associés aux technologies numériques qui relèvent de catégories spécifiques et sont liés aux moyens ou organismes inclus dans le périmètre. En vertu de la loi, tout exploitant souhaitant acquérir des biens de ce type doit en informer le Centre national d'évaluation et de certification, qui peut réaliser une évaluation préliminaire, imposer diverses conditions et exiger que le matériel ou le logiciel concerné fasse l'objet de tests. Dans ce dernier cas, l'appel d'offres devra inclure une clause suspendant toute politique d'annulation et stipulant les prescriptions à respecter ou la nécessité d'obtenir un résultat positif aux tests prévus par le Centre national ;

– Des inspections et des sanctions au sein du secteur public et du secteur privé, dont sont respectivement responsables la Présidence du Conseil des Ministres et le Ministère du développement économique.

En cas de menace grave et imminente aux réseaux, systèmes informatiques et services d'importance pour la sécurité nationale, le Premier Ministre peut ordonner la suspension ou le retrait partiel ou total d'un ou plusieurs dispositifs ou produits installés sur un réseau ou un système déterminé. Cela peut également s'appliquer à des services. La décision fait au préalable l'objet de délibérations au Comité interministériel pour la sécurité de la République et demeure valide uniquement pour la durée nécessaire à l'élimination ou à l'atténuation de la menace, conformément au principe de proportionnalité.

• Le décret 22/2019, devenu loi 41/2019 (article 1), qui complète le décret 21/2012 dit du « pouvoir en or » et devenu loi 56/2012 relative aux pouvoirs spéciaux sur l'actionnariat dans le domaine de la défense et de la sécurité nationale, ainsi que pour les activités d'importance stratégique dans les secteurs de l'énergie, des transports et des communications, inclut les services de communication électronique à haut débit qui font appel à la technologie 5G parmi les activités d'importance stratégique pour la défense nationale et la sécurité. Selon les dispositions en vigueur, en cas d'intervention de parties extérieures à l'Union européenne, les contrats ou accords relatifs à l'acquisition de biens ou services aux fins de la planification, de l'exploitation, de l'entretien et de la gestion de réseaux associés aux services de communication électronique à haut débit fondés sur la technologie 5G, ainsi que l'acquisition de « composantes technologiques à haute intensité » aux fins susmentionnées, doivent faire l'objet d'une notification envoyée au Comité dit du « pouvoir en or », créé au sein de la Présidence du Conseil des Ministres. Si le Centre national d'évaluation et de certification détecte la présence de vulnérabilités qui peuvent compromettre l'intégrité et la sécurité des réseaux et de leurs données, il peut ainsi exprimer son veto ou imposer des conditions ou prescriptions spécifiques,

qui peuvent être modifiées ou accompagnées de mesures supplémentaires, y compris le remplacement des produits ou équipements concernés.

Cyberdéfense

Le Livre blanc sur la sécurité internationale et la défense de 2015 indique qu'il est nécessaire de protéger et de défendre le domaine informatique, y compris au moyen de la création de « capacités opérationnelles défensives spécifiques… afin de préserver le tissu politique, économique et social ». Conformément au Document de planification 2019-2021 du Ministère de la défense, le cyberespace doit être protégé et défendu contre les attaques prenant pour cible les réseaux ou services informatiques ainsi que les infrastructures critiques. Ces dernières années, le Ministère de la défense a entrepris nombre de réformes afin de renforcer sa résilience et son positionnement tout en améliorant sa protection.

Le Ministère italien de la défense a, entre autres, mis sur pied le Centre conjoint d'opérations cybernétiques, un commandement militaire chargé de planifier, d'orchestrer et de mener des cyberopérations visant à déceler et neutraliser les menaces et les attaques contre des réseaux, systèmes et services du Ministère de la défense au niveau national ainsi que dans des théâtres d'opérations à l'étranger.

Le Centre conjoint d'opérations cybernétiques a récemment été incorporé au Commandement de la composante cybernétique afin de définir une chaîne de commandement plus claire et d'assurer une plus grande efficacité et une meilleure coordination entre les départements compétents en matière de cybersécurité au sein du Ministère de la défense (aviation, armée et marine). Le Commandement appuie le Siège conjoint d'opérations italien et a pour mandat de mener des opérations défensives en vue de protéger le Ministère de la défense italien et son appareil militaire contre les incidents et attaques cybernétiques.

En outre, le Commandement de la composante cybernétique :

- est responsable de la cybersécurité et de la cyberdéfense des réseaux du Ministère de la défense ; il agit par l'intermédiaire de l'Équipe d'intervention en cas d'atteinte à la sécurité informatique, qui est chargée de superviser les activités cybernétiques et de prévenir et gérer les incidents et urgences dans le secteur de la défense ;
- mène actuellement une étude visant à définir le cadre juridique dans les théâtres opérationnels, en conformité avec le droit international et le droit international humanitaire. Cette étude a pour but de déterminer les normes et règles minimales d'engagement afin d'appuyer les opérations grâce aux activités menées dans le cyberespace. La nécessité d'élaborer un cadre juridique à cet égard émane des nombreuses activités et des multiples exercices menés au niveau national et international ces dernières années, y compris dans le cadre de OTAN.

Un cyberlaboratoire a également été créé au sein du Commandement afin d'élaborer les outils nécessaires pour enquêter sur les vulnérabilités informatiques et organiser des formations.

Avec le concours de nombreuses universités italiennes, des essais préliminaires ont en outre été réalisés afin de déterminer la portée nécessaire des formations techniques sur le cyberespace à la Faculté des télécommunications des Forces armées italiennes.

Efforts engagés au niveau national pour promouvoir la coopération internationale, y compris en ce qui concerne les rapports du Groupe d'experts gouvernementaux

En vertu de l'article 10 de la Constitution italienne, « l'ordre juridique italien se conforme aux règles du droit international généralement reconnues ».

L'Italie s'engage par conséquent à promouvoir l'application du droit international, y compris la Charte des Nations Unies dans son intégralité, dans le cyberespace et souscrit aux observations formulées par l'Union européenne dans sa contribution au présent rapport. Elle se conforme en outre aux règles, normes et principes de comportement responsable des États, qui sont énoncés dans le rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Elle est également attachée à l'élaboration de mesures de confiance et de programmes de renforcement des capacités, ainsi qu'à une gouvernance d'Internet fondée sur une approche multipartite.

L'Italie appuie l'Appel de Paris pour la confiance et la sécurité dans le cyberespace en ce qui concerne la mise en œuvre de mesures conjointes visant à atténuer les menaces pour la stabilité du cyberespace, favoriser la confiance et renforcer les capacités. Elle est également signataire de l'Appel de Christchurch visant à éliminer les contenus terroristes et extrémistes violents en ligne.

La promotion d'activités de renforcement des capacités auprès de pays tiers fait partie intégrante de la stratégie italienne de cybersécurité et se fonde sur les Conclusions du Conseil européen sur des lignes de conduite de l'Union européenne concernant le renforcement des cybercapacités externes, adoptées par le Conseil des affaires générales de l'Union européenne à sa 3629e session, le 26 juin 2018. Les activités de renforcement des capacités organisées avec des pays tiers se concentrent avant tout sur l'échange d'informations et de bonnes pratiques, notamment eu égard aux interventions d'urgence en cas d'atteinte à la sécurité informatique, ainsi que sur l'éducation et la formation.

Participer aux travaux des instances internationales et promouvoir le respect des normes de comportement responsable des États dans le cyberespace sont également un aspect fondamental de la stratégie italienne de cybersécurité. Dans le cadre de consultations ou de dialogues bilatéraux ou multilatéraux, l'Italie discute également de la coopération internationale dans le cyberespace, notamment eu égard aux rapports du Groupe d'experts gouvernementaux. Les principales instances où elle contribue activement au renforcement de la coopération sont l'Organisation des Nations Unies, l'Union européenne, l'OTAN, l'Organisation pour la coopération et la sécurité en Europe (OSCE), le Conseil de l'Europe et le Groupe des sept.

Au sujet de ce dernier, l'Italie a d'ailleurs organisé les 10 et 11 avril 2017 une réunion des ministres des affaires étrangères du Groupe des sept, qui a abouti à l'adoption de la Déclaration du Groupe des sept sur le comportement responsable des États dans le cyberespace. Dans sa déclaration, le Groupe des sept appelle tous les États à fonder leur utilisation des technologies numériques sur les rapports consécutifs du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

Quand elle a assuré la présidence de l'OSCE en 2018, l'Italie a apporté un soutien actif à la mise en pratique par les États participants des mesures de confiance de l'OSCE dans le domaine de la sécurité informatique et de la sécurité des communications. À ce titre, elle a notamment organisé des discussions fondées sur un scénario d'atteinte à la cybersécurité en marge de la Conférence de l'OSCE sur la

cybersécurité et la sécurité des technologies numériques, qui a eu lieu les 27 et 28 septembre 2018 à Rome. En 2019, dans le cadre de sa présidence du Groupe de contact asiatique de l'OSCE, l'Italie a organisé à Tokyo les 2 et 3 septembre la vingtième Conférence asiatique de l'OSCE, dont le thème était « Comment parvenir à une sécurité globale à l'ère numérique : les perspectives de l'OSCE et de ses partenaires asiatiques ». Elle a également appuyé un certain nombre de projets de renforcement des capacités de l'OSCE dans le domaine des technologies numériques et de la cybersécurité, y compris la formation sous-régionale sur le rôle des technologies numériques dans le contexte de la sécurité internationale, organisée à Athènes les 7 et 8 février 2019.

L'Italie participe activement aux activités du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et appuie les travaux de l'actuel Groupe d'experts gouvernementaux et des groupes passés. Elle rappelle également que, dans sa résolution 70/237, l'Assemblée générale a salué les conclusions auxquelles étaient parvenues les précédents groupes d'experts gouvernementaux dans leurs rapports de 2013 et 2015 et demandé aux États Membres de s'inspirer, pour ce qui touchait à l'utilisation de l'informatique et des technologies des communications, du rapport de 2015 du Groupe d'experts gouvernementaux.

La récente création d'un département compétent en matière de cybersécurité et des politiques numériques au sein du Ministère italien des affaires étrangères et de la coopération internationale est appelée à renforcer et promouvoir ses activités diplomatiques et la coopération internationale dans ce domaine.

Japon

[Original : anglais]
[31 mai 2020]

Le Japon se félicite de l'occasion qui lui est donnée de répondre à la demande formulée dans la résolution 74/28 de l'Assemblée générale, intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ».

1. Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

Efforts engagés au niveau national pour renforcer la sécurité informatique

Le Japon a jeté les bases juridiques de l'utilisation des données, notamment en adoptant la loi fondamentale sur la promotion de l'utilisation des données du secteur public et du secteur privé et la loi modifiée sur la protection des renseignements personnels. Le Gouvernement a également adopté une politique visant à créer une société anthropocentrique qui favorise à la fois le développement économique et le règlement des problèmes sociaux en intégrant pleinement le cyberespace dans l'espace réel. Dans ces circonstances, les données générées en très grand nombre par des capteurs et des dispositifs dans l'espace réel sont actuellement stockées et analysées dans le cyberespace. En outre, la fourniture dans l'espace réel de nouveaux produits et services qui apportent une valeur ajoutée grâce à l'utilisation de données est un phénomène cyclique émergeant dans de nombreux domaines. Le cyberespace et l'espace réel ne sont plus des entités indépendantes et distinctes mais bien des entités qui interagissent. Par conséquent, ils doivent être considérés comme une seule entité organique en constante évolution.

L'unification du cyberespace et de l'espace réel augmente considérablement la possibilité de vivre dans l'abondance. En même temps, elle accroît également le risque que le cyberespace soit utilisé de façon abusive par des acteurs malveillants. On prévoit une augmentation rapide et exponentielle du risque que l'espace réel subisse des pertes ou des dommages économiques et sociaux. La flambée de maladie à coronavirus (COVID-19) semble en particulier renforcer la dépendance de l'humanité vis-à-vis des technologies numériques tout en exacerbant les risques et problèmes découlant de l'utilisation de ces technologies à des fins malveillantes. Les informations faisant état de cyberattaques et d'actes de malveillance commis dans le cyberespace par des acteurs qui cherchent à tirer parti de la crise, y compris en demandant des rançons à des institutions ou autorités médicales ou en commettant des attaques, de plus en plus fréquentes, par déni de service contre des centres de recherche médicaux, sont une source de préoccupation grandissante. Dans ces conditions, la sécurité du cyberespace, qui sert de fondement à l'économie, doit être assurée et, en même temps, son évolution et son développement doivent se poursuivre de façon autonome afin de générer durablement progrès et richesses pour la société.

Certains pays ont récemment eu tendance à réagir aux cybermenaces en mettant l'accent de façon autoritaire sur la gestion et le contrôle du cyberespace. Toutefois, une telle tendance a pour effet d'empêcher le cyberespace de se développer de façon autonome et durable. Ainsi, le cyberespace actuel, qui s'est développé grâce aux initiatives autonomes de toutes les parties prenantes, doit être respecté, et la cybersécurité doit être assurée grâce à une collaboration et à une coopération avec ces parties prenantes. Partant de ce principe et conscient des aspirations pour 2020 et au-delà, le Japon ne ménagera pas ses efforts en matière de cybersécurité et entend définir plus avant sa vision de la cybersécurité, déceler les difficultés émergentes et appliquer rapidement les mesures qui s'imposent.

Efforts engagés au niveau national pour promouvoir la coopération internationale

Étant donné que les conséquences des incidents dans le cyberespace peuvent facilement avoir des effets au-delà des frontières nationales, les cyberincidents qui surviennent à l'étranger peuvent toucher le Japon. Celui-ci collaborera avec les gouvernements et le secteur privé du monde entier pour assurer la sécurité du cyberespace et œuvrer à la fois en faveur de la paix et de la stabilité internationales et de sa propre sécurité. À cette fin, le Gouvernement contribuera activement à diverses discussions internationales et à l'échange d'informations afin d'en arriver à une compréhension commune des questions liées au cyberespace. Il partagera également son expertise avec d'autres pays, encouragera une collaboration ciblée et agira lorsqu'il y aura lieu. En outre, le Gouvernement participera activement aux discussions internationales visant à s'attaquer aux problèmes de cybersécurité qui se sont déclarés lors de la pandémie de COVID-19.

En ce qui concerne la politique de partage des compétences et de coordination, le Japon travaillera dans le cadre de dialogues bilatéraux et de conférences internationales sur la cybersécurité afin d'échanger des informations sur les politiques, les stratégies et les systèmes relatifs à la cybersécurité et utilisera ces connaissances pour élaborer sa politique de cybersécurité. Nous renforcerons également notre coopération concernant cette politique avec des partenaires stratégiques qui ont adopté les mêmes principes fondamentaux que nous en matière de cybersécurité.

Pour ce qui est de la collaboration internationale en cas d'atteinte à la cybersécurité, le Gouvernement échangera des informations sur les cyberattaques et les cybermenaces et renforcera la coopération entre les équipes d'intervention en cas

d'atteinte à la sécurité informatique afin que la réaction en cas d'incident soit bien coordonnée. Il s'emploiera également à améliorer les capacités d'intervention coordonnées en participant à des formations conjointes et à des exercices internationaux de simulation de cyberattaque. De plus, il réagira de façon appropriée à tout incident et collaborera le cas échéant avec la communauté internationale.

À la lumière des aspects diplomatiques de la coopération dans le domaine de la cybersécurité, l'engagement du Japon repose sur trois piliers : l'état de droit, les mesures de confiance et le renforcement des compétences sur le cyberespace.

Il est primordial de promouvoir l'état de droit pour assurer la paix et la stabilité internationales ainsi que la sécurité du pays. Le Japon est d'avis que le droit international existant, y compris la Charte des Nations Unies, s'applique également au cyberespace. Le Japon participera avec dynamisme aux discussions sur les applications individuelles et spécifiques du droit international existant et sur l'élaboration et l'universalisation de normes. En ce qui concerne les mesures de lutte contre la cybercriminalité, la Police nationale et les ministères et organismes compétents coopéreront afin de promouvoir plus avant les partenariats internationaux au moyen de la coopération internationale en matière d'enquête et de l'échange d'informations avec les organisations internationales, les forces de l'ordre et les organismes responsables de la sécurité informatique dans d'autres pays, en tirant parti des cadres existants tels la Convention sur la cybercriminalité, les traités d'entraide judiciaire ou encore l'Organisation internationale de police criminelle (INTERPOL).

Le Japon œuvrera au renforcement de la confiance entre États afin de prévenir les cyberattaques. En raison de l'anonymat et du secret entourant les cyberattaques, il existe des risques que celles-ci puissent exacerber involontairement les tensions entre États. Pour éviter toute confrontation accidentelle et superflue, il importe d'établir des voies de communication internationales en temps de paix, au cas où des incidents dépassant les frontières nationales surviendraient. Il est également nécessaire d'accroître la transparence et de renforcer la confiance entre les États grâce à un échange d'informations et à des dialogues politiques proactifs dans le cadre de consultations bilatérales et multilatérales. Le Gouvernement coopérera également avec d'autres États afin d'envisager la création d'un mécanisme de coordination des questions relatives au cyberespace. À cet égard, le Japon est un fervent partisan des mesures de confiance et, à ce titre, a proposé l'organisation d'une réunion intersessions du Forum régional de l'Association des nations d'Asie du Sud-Est (ASEAN) consacrée à la cybersécurité, qu'il a coprésidée. Il apporte également une assistance au renforcement des capacités à divers pays, en particulier dans la région Asie-Pacifique.

En ce qui concerne le renforcement des capacités, étant donné que l'interdépendance entre les pays s'est accrue, il n'est pas possible pour le Japon d'assurer seul la paix et la stabilité. Une coordination mondiale visant à réduire et à éliminer les vulnérabilités en matière de cybersécurité est essentielle pour assurer la sécurité du Japon. De ce point de vue, l'aide au renforcement des capacités dans d'autres États assure une stabilité pour les résidents du Japon et pour les activités à l'étranger des entreprises japonaises qui dépendent d'infrastructures critiques de même que de l'utilisation et du développement sûrs du cyberespace. En même temps, cette aide est aussi directement liée à la sécurité de tout le cyberespace et contribue à améliorer la sécurité dans le monde entier, y compris au Japon. En outre, dans le domaine de la cybercriminalité, le Japon est le premier pays d'Asie à avoir ratifié la Convention sur la cybercriminalité et joue un rôle constructif dans la promotion de cet instrument, qui constitue un cadre juridique important pour la lutte contre la cybercriminalité en apportant une aide au renforcement des capacités en Asie.

2. Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Le Japon estime qu'il est à la fois important et utile que tous les États tiennent compte des concepts suivants, énoncés par le Groupe d'experts gouvernementaux.

Répercussions sur la communauté internationale des actes malveillants commis dans le cyberespace

Pour intégrer avec souplesse l'évolution des technologies numériques dans nos vies et prévenir tout préjudice découlant d'actes mal intentionnés commis dans le cyberespace, le Japon considère qu'il importe de déceler les menaces existantes et éventuelles pouvant subvenir dans le cyberespace et les répercussions qu'elles pourraient avoir pour la communauté internationale.

Application des normes facultatives et non contraignantes de comportement responsable des États

Afin d'atténuer au maximum les conséquences des actes malveillants commis dans le cyberespace et de dissuader les auteurs de tels actes, le Japon rappelle l'importance du rapport du Groupe d'experts gouvernementaux adopté par consensus, y compris les normes facultatives et non contraignantes de comportement responsable des États qui y sont énoncées. Nous devrions approfondir la discussion, en coopération avec les organisations régionales pertinentes, afin de tirer parti concrètement et efficacement de ces efforts louables.

Promouvoir l'application des normes facultatives et non contraignantes de comportement responsable des États et la coopération aux fins du renforcement de la confiance et des capacités

Afin d'appuyer les efforts engagés par les pays qui entendent créer et préserver un cyberespace libre, équitable et sûr dans le contexte de la sécurité internationale, toutes les nations devraient exprimer leur volonté d'éliminer les failles de sécurité dans le cyberespace et de prévenir la réalisation de tout profit au moyen d'actes de malveillance commis dans le cyberespace. À cette fin, les membres du Groupe devraient continuer d'encourager tous les États à mettre en œuvre sans réserve les normes facultatives et non contraignantes de comportement responsable des États, ainsi que des mesures confiance, et à coopérer afin d'appuyer le renforcement des capacités dans les différents pays et ainsi assurer l'application des normes et recommandations précédemment mentionnées, y compris lors des réunions futures du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée.

Mexique

[Original : espagnol]
[29 mai 2020]

Les progrès des technologies numériques ouvrent de nombreuses perspectives en ce qui concerne le développement durable et peuvent être un facteur de justice, d'équité et d'inclusion dans le monde. Il incombe aujourd'hui à la communauté internationale dans son entier d'en garantir l'utilisation pacifique dans l'intérêt de tous.

Les délibérations, au sein de l'ONU, sur la stabilité dans le cyberespace, la cybersécurité et la gouvernance du cyberespace, et en particulier les rapports produits par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de

l'informatique et des télécommunications dans le contexte de la sécurité internationale, travaux qui visent à favoriser le comportement responsable des États dans le cyberespace, tracent la voie vers un cyberespace ouvert, libre, stable et sûr.

C'est dans ce contexte que le Gouvernement mexicain soumet le présent rapport. Il est convaincu de la valeur des résolutions adoptées par l'Assemblée générale sur ce sujet et du caractère inéluctable de la voie multilatérale, seule à même de garantir, dans une vision à long terme, les utilisations légitimes et pacifiques du cyberespace, la résilience dans l'environnement numérique, le potentiel des technologies numériques en tant que facteur de développement durable et la protection des droits de l'homme dans le cyberespace.

1. Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

S'agissant de la sécurité de l'information et des équipes d'intervention, le Gouvernement mexicain a consolidé les mécanismes nationaux de coordination suivants :

a) Comité spécial sur la sécurité de l'information

Organisme collégial interinstitutionnel, il est chargé d'élaborer une politique de sécurité de l'information applicable aux organismes de sécurité nationale et d'en vérifier la bonne application au Mexique. Il réunit les institutions fédérales mexicaines chargées de la sécurité nationale, de la sécurité publique, des télécommunications, du secteur financier et de la politique étrangère. Le Comité centralise, entre autres activités, la conception et la mise à jour de la stratégie nationale de cybersécurité, des exercices d'intervention en cas d'incidents informatiques et l'exécution d'activités de sensibilisation à la sécurité de l'information.

b) Centre national d'intervention en cas d'incident cybernétique

Le centre, qui relève de la nouvelle Garde nationale mexicaine, est chargé de surveiller l'intégrité de l'infrastructure technologique stratégique du pays. Spécialisé dans la prévention et les enquêtes sur les actes illicites commis par voie informatique, il surveille les réseaux pour identifier les comportements délictueux et mène des activités de cybersécurité visant à réduire et atténuer les risques de menaces et de cyberattaques. Il exécute également des programmes de développement scientifique et technologique dans le domaine de la cybernétique.

c) Groupe d'intervention en cas d'atteinte sensible à la sécurité de l'information

Le groupe, mécanisme de coordination visant à améliorer l'efficacité des interventions en cas d'atteinte à la sécurité de l'information dans le secteur financier, rassemble le Bureau du Procureur, les autorités financières nationales et les associations professionnelles financières du Mexique ; il est chargé des incidents affectant directement le secteur financier.

Au niveau national, le Mexique a pris ces dernières années les mesures ci-après pour renforcer la sécurité de l'information :

Le Gouvernement mexicain, ou plus précisément le Ministère de la sécurité et de la protection publique, organise chaque année une Semaine nationale de la cybersécurité. Espace de dialogue et de promotion de la cybersécurité, cette manifestation vise à coaliser les secteurs concernés pour préserver un environnement numérique sûr et résilient. Elle est également l'occasion d'activités de sensibilisation publique aux technologies de l'information et à la sécurité numérique, conférences,

tables rondes, cours de formations, ateliers, séminaires sur Internet ou activités ludiques.

Depuis 2018, le Gouvernement mexicain, en partenariat avec l'Organisation des États américains (OEA) et Trend Micro, organise un événement annuel intitulé « Cyberwomen Challenge », qui vise à promouvoir l'égalité des genres dans tout ce qui a trait à la protection et la lutte contre les menaces de cybersécurité et à constituer ou consolider des capacités institutionnelles dans ce domaine.

En 2019, le Ministère des communications et des transports a coordonné l'organisation de groupes de travail sur la cybersécurité, auxquels ont participé plus de 5 000 agents des centres d'inclusion numérique relevant de ce ministère. L'objectif était de mettre en lumière les comportements à risque dans l'utilisation des services de télécommunications et de radiodiffusion. Les informations recueillies dans le cadre de cette activité ont servi de base au rapport intitulé « Hábitos de los usuarios en ciberseguridad en México 2019 ».

Sur la base des résultats de ce rapport, un simulateur a été développé avec le soutien de l'OEA et du Gouvernement du Royaume-Uni. L'outil donne aux participants la possibilité de faire l'expérience, dans un environnement interactif et sous une forme mise en scène, des menaces contre la cybersécurité, cette technique permettant d'observer leur capacité à y faire face et de leur donner des conseils sur les meilleurs moyens de se protéger.

En outre, dans le souci d'œuvrer au renforcement de la coopération internationale et du comportement responsable des États dans le cyberespace, le Mexique participe aux forums, mécanismes et initiatives multilatéraux et régionaux suivants :

a) Première Commission de l'Assemblée générale des Nations Unies

Le Mexique fait partie du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé par la résolution 73/27 de l'Assemblée générale.

L'un de ses experts participe par ailleurs au Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, créé en application de la résolution 72/266.

Le Mexique a cherché à concilier les deux processus, qui se fondent tous deux sur les travaux des groupes d'experts antérieurs et sur les rapports adoptés par consensus par l'Assemblée générale.

b) Groupe des Amis des technologies numériques

Le Mexique tient à prendre part, à titre d'initiateur ou de participant, à des projets liés aux technologies numériques axés en particulier sur la bonne utilisation des technologies numériques au service des objectifs de développement durable et des cibles qui y sont associées. Dans cet esprit, le Mexique copréside depuis novembre 2019, avec la Finlande et Singapour, le Groupe des Amis des technologies numériques, qui vise à promouvoir un dialogue inclusif avec toutes les parties prenantes portant, d'une part, sur l'étude des liens entre les technologies numériques et le développement durable et, d'autre part et de manière transversale, de la coopération internationale en la matière.

c) Groupe de haut niveau sur la coopération numérique

Comme suite aux recommandations du Groupe de haut niveau sur la coopération numérique, le Mexique a dirigé avec l'Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes (ONU-Femmes) un groupe chargé de proposer des mesures spécifiques d'application des recommandations 1C et 1D, sur l'inclusion numérique et les mesures connexes.

d) Union internationale des télécommunications

Le Mexique participe aux initiatives que l'Union internationale des télécommunications coordonne en matière de sécurité de l'information et de cybersécurité, telles que le Programme mondial cybersécurité et l'Indice de cybersécurité dans le monde.

Le Mexique attache une importance particulière à la première de ces initiatives, qui, d'une part, contribue à la construction d'un environnement numérique plus sûr et plus résistant, mais présente d'autre part un intérêt intrinsèque en ce qu'elle permet de rassembler tous les acteurs concernés, à savoir les États, le secteur privé, la société civile et les universités.

e) Organisation des États américains

Le Mexique participe et collabore activement au programme de cybersécurité du Comité interaméricain contre le terrorisme de l'OEA, programme qui vise à l'élaboration de politiques, au renforcement des capacités, à la recherche et la sensibilisation à la cybersécurité dans les Amériques.

Le Centre national d'intervention en cas d'atteinte à la sécurité informatique fait par ailleurs partie du réseau hémisphérique des équipes d'intervention des Amériques, qui relève lui-même de ce programme de cybersécurité.

Le Mexique participe également au groupe de travail sur les mesures de coopération et de confiance dans le cyberespace du Comité interaméricain contre le terrorisme de l'OEA. À l'issue de ses travaux, le Groupe, créé en 2018, a préconisé les mesures de confiance suivantes :

- Fournir des informations sur les politiques nationales en matière de cybersécurité telles que stratégies nationales, livres blancs, cadres juridiques et autres textes jugés pertinents par tel ou tel État ;
- Désigner un point de contact national au niveau politique pour discuter des conséquences des menaces numériques dans l'hémisphère ;
- Désigner au Ministère des affaires étrangères, si ce n'est pas déjà fait, des points de contact devant faciliter, à l'échelle internationale, la coopération et les dialogues sur la cybersécurité et le cyberespace ;
- Développer et renforcer les capacités par le biais d'activités telles que séminaires, conférences et ateliers sur la diplomatie numérique, organisées au profit des fonctionnaires publics et privés ;
- Encourager la prise en compte des questions de cybersécurité et du cyberespace dans les cours de formation de base et de formation des diplomates et des fonctionnaires des ministères des affaires étrangères et autres services de l'État ;
- Promouvoir la coopération et la mise en commun des meilleures pratiques en matière de diplomatie numérique, de cybersécurité et de cyberespace par la création de groupes de travail et d'autres mécanismes de dialogue et grâce à la signature d'accords entre États.

f) Forum mondial sur la cyberexpertise

Le Mexique participe depuis 2015 à ce forum qui vise à renforcer les capacités en matière de cybersécurité. Il s'intéresse en particulier à la prévention des cyberattaques, à la protection des données, à la prévention de la cybercriminalité (y compris la pédopornographie et infractions connexes), aux mesures d'administration en ligne et stratégies numériques, à la protection des infrastructures critiques, aux utilisations pacifiques des TIC et de l'internet et l'applicabilité du droit international au cyberespace.

g) Forum des équipes d'intervention en cas d'incidents liés à la sécurité informatique

Le Centre national d'intervention en cas d'incident cybernétique fait partie du Forum of Incident Response and Security Teams, un forum mondial de collaboration rassemblant les équipes d'intervention du monde entier en cas d'incidents cybernétiques. Cette structure permet de faire naître ou progresser des enquêtes menées en collaboration avec les unités compétentes des services de police d'autres pays, qui permettent de détecter et de localiser les auteurs probables de cyberattaques.

2. Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Le Mexique considère que, comme l'a affirmé le Groupe d'experts gouvernementaux dans ses précédents rapports, le droit international est applicable au cyberespace. Cherchant à donner corps à cette idée, le Gouvernement mexicain s'est employé, au plan interne, à définir sa position quant au droit international applicable, à savoir la Charte des Nations Unies, le droit international des droits de l'homme, le droit international humanitaire, les normes applicables du droit international coutumier et la jurisprudence connexe.

Dans la droite ligne des rapports précédents du Groupe d'experts gouvernementaux, le Mexique reconnaît le rôle moteur que les organisations régionales peuvent jouer dans ce domaine, en particulier dans la mise en œuvre des mesures de confiance. Fort de cette conviction, le Gouvernement a encouragé ses organes nationaux à envisager de donner suite aux mesures de confiance prévues dans les rapports du Groupe d'experts gouvernementaux puis étoffées dans le cadre des travaux de l'OEA.

Le concept de renforcement des capacités, tel qu'il ressort desdits rapports, revêt aux yeux du Mexique une importance particulière, dans la mesure où il englobe non seulement le développement des capacités nationales dans le domaine de la sécurité de l'information, mais aussi le recours impératif à toutes les modalités de coopération internationale, dont la contribution à la paix et à la sécurité internationales n'est plus à démontrer. Le renforcement des capacités permet aux États et à l'ensemble des parties prenantes de s'équiper pour faire face aux cybermenaces et permet de faire émerger des positions communes sur les différents enjeux de cybersécurité.

Au cours de la période considérée, le Gouvernement mexicain a donc également cherché à promouvoir les synergies entre les différents groupes, forums, organes et initiatives du système des Nations Unies compétents en matière de technologies numériques, de télécommunications, de cybersécurité, de gouvernance du cyberespace, de coopération numérique et de transformation technologique, l'objectif étant de parvenir à une plus grande cohérence, d'éviter les chevauchements et de mieux utiliser les ressources de la coopération.

Singapour

[Original : anglais]
[27 avril 2020]

Singapour est fermement attaché à l'établissement d'un ordre international fondé sur des règles dans le cyberespace, source de confiance entre les États Membres et vecteur de progrès économique et social. Si elle souhaite tirer pleinement parti des technologies numériques, la communauté internationale devra mettre en place un cyberespace sûr, fiable et ouvert, qui reposera sur les normes de droit international applicables à cet espace, des normes bien définies régissant le comportement responsable des États et des mesures de confiance efficaces, accompagnées d'actions coordonnées de renforcement des capacités. Il est important que l'on poursuive les discussions relatives à ces lois, règles et normes dans le cadre de l'ONU – seule instance universelle, inclusive et multilatérale, où tous les États ont voix au chapitre.

Singapour participe à la fois au Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Il réaffirme que les deux plateformes sont à ses yeux complémentaires et continuera d'y contribuer de manière constructive. Leur travaux ne pourront être menés à bon port qu'au prix d'un esprit de coopération constructive, de consensus, de respect mutuel et de confiance mutuelle. En tant que coprésident, avec l'Estonie, du Groupe des Amis sur la gouvernance électronique et la cybersécurité, Singapour est déterminé à rallier tous les pays à ces deux processus. Il voit dans la réunion consultative intersessions informelle du Groupe de travail à composition non limitée, présidée par le Directeur général de l'Office de la cybersécurité de Singapour, David Koh, une occasion intéressante de faciliter un échange interactif entre les États Membres, le secteur privé, la société civile, les universités et la communauté technique sur une série de questions de fond.

Singapour estime que les États doivent promouvoir la sensibilisation aux normes facultatives et non contraignantes existantes en matière de comportement responsable des États et soutenir leur mise en œuvre. Il est favorable, le cas échéant, à une élaboration plus poussée des normes. Par exemple, les infrastructures d'information critiques supranationales pourraient être considérées comme une catégorie d'infrastructures critiques à part, dont la protection relèverait de la responsabilité partagée de tous les États Membres, ce qui pourrait être incorporé à l'ensemble des normes existantes[11].

Les organisations régionales sont appelées à jouer un rôle de plus en plus important. L'Association des nations de l'Asie du Sud-Est (ASEAN) a réaffirmé la nécessité d'un ordre international fondé sur des règles dans le cyberespace dans la première déclaration des dirigeants de cette organisation sur la coopération en matière de cybersécurité, publiée en avril 2018. En septembre 2018, les participants à la troisième Conférence ministérielle de l'ASEAN sur la cybersécurité ont approuvé le principe des 11 normes énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux, et sont convenus de mettre l'accent sur le renforcement des capacités régionales dans l'application de ces normes. En octobre 2019, la quatrième Conférence ministérielle de l'ASEAN sur la cybersécurité a décidé de créer un comité de travail chargé d'envisager l'élaboration d'un plan d'action régional à long terme

[11] Les infrastructures d'information critiques supranationales sont celles qui appartiennent à des entreprises privées, dont les opérations dépassent les frontières nationales et sur lesquelles aucun État n'exerce une juridiction exclusive.

visant à assurer une application efficace et concrète des normes, notamment dans les domaines de la coopération entre les équipes d'intervention en cas d'atteinte à la sécurité informatique, de la protection des infrastructures d'information critiques et de l'entraide en matière de cybersécurité.

Il est essentiel de renforcer les capacités des États pour qu'ils soient en mesure d'appliquer les règles et normes de comportement responsable. À cet effet, Singapour a mis en place en 2016 dans le cadre de l'ASEAN un programme de renforcement des cybercapacités, doté d'un budget de 10 millions de dollars singapouriens et destiné à mettre les États membres mieux à même d'adopter des stratégies et politiques en la matière et de faire face aux questions techniques y relatives. À ce jour, 170 fonctionnaires des États membres ont été formés dans ce cadre. Dans le prolongement de cette initiative, Singapour a lancé en octobre 2019 le Centre d'excellence pour la cybersécurité, fruit d'un partenariat avec l'ASEAN, financé à hauteur de 30 millions de dollars singapouriens et destiné à renforcer les capacités des États membres de l'organisation en matière d'élaboration de politiques et de stratégies de cybersécurité et leurs capacités techniques et opérationnelles dans ce domaine et à favoriser une collaboration plus étroite avec les partenaires internationaux.

Singapour a également coorganisé, dans le cadre d'un cyberprogramme issu d'un partenariat avec l'ONU, un atelier visant à faire mieux connaître dans les États membres de l'ASEAN les normes applicables au cyberespace et les mécanismes de planification des scénarios relatifs à cet espace. En outre, Singapour s'est associé au Bureau des affaires de désarmement pour développer un cours de formation en ligne phare ouvert à tous les États Membres de l'ONU. Le cours vise à promouvoir une meilleure compréhension de l'utilisation des technologies numériques et de leurs implications pour la sécurité internationale. Singapour a également mis en place plusieurs cours de formation sur la cybersécurité dans le cadre de son programme de coopération. Il reste déterminé à partager son expérience et ses compétences avec les États Membres de l'ONU, en particulier les petits pays et les pays en développement.

À l'échelle nationale, Singapour a continué de renforcer la cybersécurité de ses systèmes et réseaux, et notamment sur trois fronts : la construction d'une infrastructure résiliente, la création d'un cyberespace plus sûr et la mise au point d'un écosystème de cybersécurité dynamique :

a) La construction d'une infrastructure résiliente. L'Agence de cybersécurité de Singapour a mis au point un Plan directeur opérationnel de cybersécurité qui s'inscrit dans le droit fil des efforts constamment déployés dans le pays pour donner aux secteurs d'infrastructures d'information critiques du pays les moyens de fournir les services essentiels de manière plus sûre et résiliente. Ce Plan a pour fonction d'amplifier les efforts intersectoriels d'atténuation des cybermenaces dans l'environnement technologique opérationnel et de renforcer les partenariats avec l'industrie et les parties prenantes. Il s'articule autour de six grandes initiatives englobant les enjeux humains, logistiques et technologiques et destinées à renforcer les capacités des propriétaires des infrastructures d'information critiques et des organisations qui utilisent des systèmes de technologies opérationnelles.

b) La création d'un cyberespace plus sûr. Dans le cadre des efforts de sécurisation et d'assainissement du cyberespace, Singapour introduira en 2020 un programme de labellisation des appareils intelligents connectés au réseau du point de vue de la cybersécurité. La participation au programme sera dans un premier temps facultative, l'idée étant de laisser le temps au marché et aux développeurs d'en apprécier l'utilité. Le label classe les produits en fonction de leur degré de sécurité par défaut, le consommateur étant alors à même de choisir le produit le mieux coté. Il s'agit par là d'inciter les fabricants à mettre au point et à offrir des produits aux fonctionnalités de cybersécurité améliorées et répertoriées.

c) La mise au point d'un écosystème de cybersécurité dynamique. Singapour est conscient que l'on ne peut renforcer la cybersécurité sans mettre au point un cyberécosystème ni encourager l'innovation dans ce secteur. Il est également de plus en plus nécessaire de constituer un vivier de talents capables d'assumer des responsabilités en matière de cybersécurité dans les organisations. Depuis sa création en 2015, l'Agence de cybersécurité a travaillé avec des agences gouvernementales, des associations, des partenaires industriels et des établissements d'enseignement supérieur du pays pour élargir et développer les ressources humaines dans le domaine. C'est sous son égide que le pays a lancé une nouvelle initiative, SG Cyber Talent, qui vise à faire naître des vocations dès le plus jeune âge, à attirer des talents et à aider les professionnels à approfondir leurs compétences en la matière. La cible visée est d'au moins 20 000 personnes sur une période de trois ans.

Turquie

[Original : anglais]
[22 mai 2020]

Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale

Les technologies numériques sont devenues un élément essentiel de la société et de l'économie. Intégrées à un vaste réseau intéressant aussi bien le secteur public que privé et les infrastructures critiques que les particuliers, elles se sont généralisées en Turquie comme dans le reste du monde. À ce titre, elles tiennent une place de choix dans la croissance et le développement durable. Plus leur utilisation se généralise, plus elles deviennent indispensables, le collectif s'exposant ainsi à une série de risques. Les particuliers, les entreprises, les infrastructures critiques et les États sont confrontés à de graves problèmes liés aux cybermenaces.

Le premier souci de la Turquie est de prendre les mesures nécessaires pour améliorer la cybersécurité nationale. Le Ministère des transports et des infrastructures est l'organe chargé de l'élaboration des politiques et du développement des stratégies et des plans d'action concernant la cybersécurité nationale dans le pays. C'est sous la coordination du Ministère qu'ont été élaborés une stratégie et un plan d'action nationaux, avec la participation de toutes les parties prenantes, réunies dans des groupes d'étude. La stratégie nationale de cybersécurité, le plan d'action 2013-2014 et la stratégie nationale de cybersécurité 2016-2019 et le plan d'action ont déjà été publiés et mis en application. La prochaine stratégie nationale de cybersécurité et le plan d'action correspondant, portant sur la période 2020-2023, sera publiée prochainement.

Les principaux objectifs stratégiques inscrits dans le texte sont les suivants :

- protection des infrastructures critiques et renforcement de la résilience ;
- renforcement des capacités ;
- sécurité des nouvelles technologies (Internet des objets, 5G, *cloud computing*, etc.) ;
- lutte contre la cybercriminalité ;
- développer et encourager les technologies nationales ;
- réseau organique de cybersécurité ;
- renforcement de la coopération internationale.

En outre, l'équipe d'intervention en cas d'atteinte à la sécurité informatique, qui relève de l'Autorité des technologies numériques, coordonne la réaction aux cyberincidents en Turquie depuis 2013. L'équipe est chargée de la détection des cybermenaces et la réponse aux incidents cybernétiques, y compris avant, pendant et après les incidents, mais aussi des mesures préventives et de la cyberdissuasion. Ses principaux domaines d'intervention en matière de cybersécurité sont les suivants : renforcement des capacités, les mesures technologiques, la collecte et le partage de renseignements sur les menaces et la protection des infrastructures critiques.

Dans l'intérêt de la cybersécurité du pays, 14 équipes sectorielles d'intervention spécialisées dans certains secteurs ou infrastructures critiques (énergie, santé, banque et la finance, gestion de l'eau, communications électroniques et services publics critiques) et 1 299 équipes institutionnelles d'intervention en cas d'atteinte à la sécurité informatique ont également été créées depuis 2013. Toutes ces équipes, actives 24 heures sur 24 et sept jours sur sept, sont chapeautées par l'équipe nationale, l'objectif étant de réduire les risques informatiques et de lutter contre les cybermenaces.

L'équipe d'intervention en cas d'atteinte à la sécurité informatique organise et soutient des cours de formation, des universités d'été et des compétitions sur la cybersécurité qui sont ouverts à plusieurs groupes. En outre, elle propose des cours de formation à l'intention des équipes d'intervention dans divers domaines, par exemple l'analyse des logiciels malveillants ou de journaux de sécurité. Plus de 4 500 personnes ont été formées dans différents domaines de la cybersécurité par l'équipe nationale d'intervention au cours des trois dernières années.

Les études dans le domaine des mesures technologiques portent sur les activités de détection précoce, d'alarme et d'alerte. La Turquie a développé à cet effet des systèmes de détection et de prévention, qui contribuent grandement à améliorer le niveau national de cybersécurité.

Plusieurs organisations, institutions, universités et organisations non gouvernementales turques, ainsi que des acteurs du secteur privé, organisent également des séminaires, des conférences et des cours de formation dans tout le pays sur la cybersécurité, la protection des infrastructures critiques et d'autres sujets connexes.

La Turquie tient en outre une journée annuelle de la sécurité sur Internet, à l'occasion de laquelle sont organisées des activités de sensibilisation à l'utilisation éclairée et sûre de l'Internet. Une ligne d'assistance téléphonique et un site Web sécurisé, où les familles peuvent trouver des conseils pour une utilisation efficace de l'Internet, ont été lancés (https://www.guvenlinet.org.tr/).

Sachant que les particuliers sont de plus en plus nombreux à utiliser les technologies numériques, les informations et données à caractère personnel sont devenues une cible alléchante pour les auteurs de cyberattaques. La vie privée et la protection des données personnelles figurent également parmi les principales préoccupations en matière de sécurité. La loi nº 6698 sur la protection des données personnelles, entrée en vigueur en 2016, vise à cet égard à protéger la vie privée.

La Turquie a joué un rôle important dans de nombreuses organisations, soit en tant que membre fondateur, soit en tant qu'elle contribue aux actions de coopération en matière de cybersécurité et de sécurité de l'information. Elle tient ainsi au partage d'informations avec différents pays et organisations dans un large éventail de domaines. Son équipe d'intervention en cas d'atteinte à la sécurité informatique est membre de l'organisation Forum of Incident Response and Security Teams, du service Trusted Introducer, de l'Union internationale des télécommunications (UIT), de la Plateforme multinationale d'échange d'informations sur les logiciels malveillants de

l'Organisation du Traité de l'Atlantique Nord (OTAN) et du consortium Cybersecurity Alliance for Mutual Progress. La Turquie participe également au Centre d'excellence pour la cyberdéfense coopérative de l'OTAN en tant que pays parrain depuis novembre 2015. Au plan de la coopération bilatérale et multilatérale, elle a signé des protocoles d'accord avec de nombreux pays. En outre, elle participe et contribue activement aux études d'organisations internationales telles que l'OTAN, l'ONU, l'Organisation pour la sécurité et la coopération en Europe, l'Organisation de coopération et de développement économiques, le Groupe des 20, le Conseil de coopération des États de langue turcique et le Centre RACVIAC de coopération en matière de sécurité.

Les exercices de cybersécurité sont une autre activité importante de coopération et de préparation. Ces exercices, réalisés à l'échelle nationale et internationale, contribuent à sécuriser le cyberespace et permettent de mettre à l'essai les mesures conçues pour contrer les cybermenaces potentielles. Depuis 2011, quatre exercices nationaux et deux internationaux de cybersécurité ont été organisés par le Ministère des transports et de l'infrastructure. Plus récemment, Cyber Shield 2019, qui est un exercice international de cybersécurité, a été organisé conjointement par le Ministère des transports et des infrastructures et l'Autorité des technologies de l'information et de la communication le 19 décembre 2019 à Ankara, en Turquie. Cyber Shield 2019 a reçu le soutien de l'UIT et de la Cyber Security Alliance for Mutual Progress (Alliance de cybersécurité pour le progrès mutuel). En outre, la Turquie participe et contribue aux exercices internationaux de cybersécurité, par exemple, dans le cadre de l'OTAN, Locked Shields, Cyber Coalition ou l'exercice de gestion de crise.

Elle a en outre signé la Convention sur la cybercriminalité, qui couvre diverses infractions, telles que celles commises sur Internet et d'autres réseaux informatiques, la fraude informatique, la pédopornographie ou encore les atteintes à la sécurité des réseaux.

La paix et la sécurité internationales dans le cyberespace exigent des études supplémentaires fondées sur une coopération internationale renforcée. Il est évident que le droit international et les normes et règles énoncées dans les rapports du Groupe d'experts gouvernementaux et dans les études connexes contribuent à un cyberespace plus sûr.

Il est de même essentiel, pour lutter contre les cybermenaces, d'améliorer la collaboration et de soutenir les mécanismes de partage d'informations, qui doivent être considérés comme une priorité.

Il importe également d'être attentifs au besoin d'orientations sur la sécurité des technologies de nouvelle génération (Internet des objets, 5G, cloud computing, etc.). Des guides ou recommandations de référence en matière de sécurité pour les technologies de nouvelle génération, préparés en coopération entre les États Membres, contribueront à accroître le niveau de préparation aux cybermenaces associées à ces technologies. Au même titre que les études destinées au renforcement des capacités ou à l'élaboration d'orientations, les exercices internationaux de cybersécurité sont fondamentaux pour que chacun, dans le monde entier, soit mieux préparé et mieux à même de faire face aux incidents cybernétiques.

Ukraine

[Original : anglais]
[29 mai 2020]

Depuis le début de l'agression hybride menée par la Fédération de Russie contre l'Ukraine, de nouvelles menaces et de nouveaux défis sont apparus, au nombre

desquels figurent en bonne place l'utilisation de mécanismes de cyberinfluence contre la sécurité de l'État ukrainien.

L'Ukraine reste inébranlable dans son attachement au droit international régissant l'utilisation des technologies numériques et dans son soutien total aux conclusions et recommandations contenues dans les rapports du Groupe d'experts gouvernementaux. Il en va en effet de la préservation de l'égalité souveraine des États, du non-recours à la force ou à la menace de recours à la force contre l'intégrité territoriale des États, de la non-ingérence dans les affaires intérieures d'autres États et du respect des droits de l'homme et des libertés fondamentales.

Dans le souci d'organiser efficacement la lutte contre les menaces dans le cyberespace et la réglementation juridique du comportement dans cet espace et de structurer dans les grandes lignes l'action publique à cette fin, un certain nombre de règlements ont été adoptés, au nombre desquels la stratégie de cybersécurité de l'Ukraine approuvée par le Conseil national de sécurité et de défense, la décision sur la stratégie de cybersécurité de l'Ukraine (décret n° 96 du Président de l'Ukraine, en date du 15 mars 2016) et la loi sur les principes fondamentaux du maintien de la cybersécurité de l'Ukraine du 5 mai 2017.

À ces mécanismes s'ajoute l'application de certaines dispositions de la loi ukrainienne sur les sanctions du 14 août 2014, qui a permis d'organiser rapidement la riposte rapide aux menaces détectées, une série de mesures restrictives étant imposées à plusieurs personnes morales et physiques associées à des atteintes à la sécurité nationale.

Aujourd'hui, la cyberprotection des ressources d'information électroniques de l'État et des infrastructures critiques ukrainiennes est régie par la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine. La loi définit les pouvoirs, les attributions et les fonctions des acteurs de la cybersécurité et établit ainsi un système de cybersécurité structuré.

Les politiques publiques concernant la cybersécurité et la cyberdéfense ont pour fil rouge l'élaboration d'un cadre réglementaire conforme aux approches et aux normes internationales. C'est à cet objectif que répondent notamment les mesures suivantes :

- Adoption de la résolution du Gouvernement ukrainien portant approbation des conditions générales de cyberprotection des infrastructures critiques ; la démarche définie dans ce texte prend en compte les normes internationales dans le domaine de la sécurité de l'information et suit les directives de l'Union européenne, l'Ukraine participant ainsi sur un pied d'égalité à l'espace de sécurité mondial.
- Élaboration de projets de résolution du Gouvernement ukrainien portant respectivement approbation :
  - de la procédure de révision du statut de la cyberprotection des infrastructures d'information critiques, des ressources publiques d'information et des informations dont la protection est requise par la loi ;
  - de la procédure de désignation des infrastructures critiques ;
  - de la procédure d'établissement d'un registre des infrastructures d'information critiques, d'inscription de ces infrastructures audit registre et de ses modalités de création et de fonctionnement, compte tenu des prescriptions fixées dans la Directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures visant à assurer un niveau

commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union ;

– du protocole régissant les interventions menées conjointement par les entités responsables de la cybersécurité et des propriétaires (gestionnaires) d'infrastructures d'information critiques et destinées à détecter et prévenir les cyberattaques et cyberincidents ou à y mettre fin.

Afin d'améliorer le système de protection technique et cryptographique de l'information, un plan de réforme de la protection de l'information, visant à adapter la législation ukrainienne aux normes du droit européen, a été adopté. Un projet de loi sur la sécurité de l'information et les systèmes de communication et d'information a été élaboré aux fins de son application.

Pour garantir le développement efficace du système national de cybersécurité, il importe notamment de faire le point sur la situation. Ce bilan pourra conduire à remettre à neuf ou adapter la stratégie nationale de cybersécurité, à améliorer la réglementation encadrant les entités responsables de la cybersécurité, à financer des mesures de cyberprotection pour les ressources informatiques de l'État et les infrastructures critiques, à mieux former les ressources humaines qui interviennent dans le domaine de la cybersécurité, à adopter de nouvelles approches pour la coopération entre les secteurs public et privé dans ce domaine, à renforcer l'échange d'informations entre les acteurs de la cybersécurité et à resserrer les liens de collaboration qu'ils entretiennent pour régler les questions de sécurité.

Par ailleurs, afin de renforcer la sécurité de l'information et de promouvoir la coopération internationale dans ce domaine, le Service des communications spéciales de l'État a pris les mesures suivantes :

- la constitution de l'équipe d'intervention en cas d'atteinte à la sécurité informatique de l'Ukraine, qui est accréditée par le Forum of Incident Response and Security Teams et qui collabore avec d'autres équipes de 96 États ;
- le contrôle par l'État de la protection du cyberespace et de la protection technique des ressources informatiques et des informations de l'État, qui sont exigées par la loi ;
- la participation aux réunions des points de contact nationaux en passant par le réseau de communication de l'Organisation pour la sécurité et la coopération en Europe (OSCE) ;
- la sensibilisation du public et l'organisation de séminaires pratiques sur la cybersécurité au profit des acteurs du système national de cybersécurité ;
- la collaboration avec les forces de l'ordre et la communication en temps utile des informations relatives aux cyberattaques ;
- la coordination, l'organisation et l'exécution d'un audit de la communication et des systèmes technologiques des infrastructures critiques, ainsi que d'un audit de la sécurité de l'information, conformément à la norme nationale ISO/IEC 27001 de 2015.

Face aux défis et aux menaces actuels, des mécanismes juridiques sont mis en place dans le domaine de la cyberdéfense, dont les objectifs sont les suivants :

- le renforcement de la sécurité des réseaux et des systèmes d'information, qui ont vocation à protéger efficacement les informations et les données et à assurer la stabilité des réseaux et des systèmes et la continuité de leurs fonctions, ainsi que l'efficacité de la détection, de la riposte et de l'optimisation de la récupération en cas de cyberincident ;

- la mise en service d'un système de gestion des risques ;
- la création de conditions propices à la mise à disposition de ressources, y compris de ressources humaines dans le domaine de la cybersécurité ;
- le renforcement de la résilience opérationnelle et numérique des infrastructures critiques ;
- la mise sur pied d'un système de conservation des ressources informatiques de l'État et la protection des informations technologiques essentielles au fonctionnement des infrastructures critiques ;
- la participation au Comité des critères communs après signature de l'accord pertinent (Arrangement de reconnaissance mutuelle selon les critères communs dans le domaine de la sécurité numérique), qui garantira l'inscription des produits certifiés en Ukraine au registre reconnu par les pays de l'Union européenne et d'autres pays chefs de file dans ce domaine ;
- le respect scrupuleux des prescriptions de la législation relative à la protection des ressources informatiques de l'État, à la protection cryptographique et technique des informations, y compris la protection des données personnelles, par les responsables des organismes chargés de la gestion des infrastructures informatiques critiques ;
- le recours aux partenariats public-privé et à la collaboration des parties prenantes pour résoudre les problèmes liés à la cyberdéfense et la cybersécurité ;
- le relèvement du niveau général de comportement sur Internet ;
- la participation active aux initiatives pertinentes de la communauté internationale et l'adhésion aux structures compétentes des principales organisations internationales.

De 2015 à 2020, le Conseil national de défense et de sécurité a adopté des décisions annuelles sur l'application de mesures économiques spéciales et autres mesures restrictives (sanctions) contre des personnes, auxquelles ont donné effet les décrets présidentiels correspondants.

De plus, étant l'une des principales entités responsables de la cybersécurité, les services de sécurité ukrainiens prennent, en vertu des compétences que la loi leur attribue, des mesures pour améliorer le cadre réglementaire national régissant le cyberespace. Des travaux sont notamment menés régulièrement pour arrêter les règlements nécessaires à l'application de la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine.

Des mesures sont prises pour appliquer les dispositions de ladite loi au cadre réglementaire régissant les activités des services de sécurité.

Cependant, malgré ces mesures, la question de l'amélioration du cadre réglementaire dans le domaine de l'information et de la cybersécurité reste d'actualité.

En particulier, plusieurs initiatives législatives relatives aux services de sécurité, dont étaient saisies les commissions de la Verkhovna Rada de la législature précédente, n'ont pas encore été examinées par les parlementaires (renforcement de la responsabilité pénale en matière de cybercriminalité, répartition des pouvoirs d'enquête entre les services de sécurité et la Police nationale et détermination des responsabilités en cas de non-respect).

Les dispositions de la Convention sur la cybercriminalité n'ont pas encore été pleinement mises en œuvre.

La Convention sur la cybercriminalité du Conseil de l'Europe datant du 23 novembre 2001 a été ratifiée par la Verkhovna Rada en septembre 2005. Ses dispositions couvrent la responsabilité pénale pour les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques, à savoir : l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système, l'abus de dispositifs. En d'autres termes, elles couvrent les infractions liées aux atteintes au fonctionnement durable des infrastructures critiques.

Toutefois, plusieurs dispositions de la Convention ne sont pas traduites dans la législation nationale à l'heure actuelle, ce qui entrave le travail de détection et de prévention de la cybercriminalité effectué par les services de détection et de répression. Celles qui doivent encore être transposées en droit interne portent sur la conservation rapide de données informatiques stockées, la conservation et la divulgation rapides de données relatives au trafic, l'injonction de produire, la perquisition et la saisie de données informatiques stockées et la collecte en temps réel des données relatives au trafic (articles 16 à 20). Il est également nécessaire de modifier le Code de procédure pénale ukrainien afin d'introduire une catégorie distincte de preuves : les preuves numériques.

Au sein du groupe de travail relevant de la commission parlementaire sur l'application des lois, les représentants des services de sécurité élaborent actuellement un projet de loi sur les amendements à apporter à certains textes relatifs à la mise en œuvre de la Convention sur la cybercriminalité. Il s'agit de traduire les dispositions de la Convention dans la législation ukrainienne, d'améliorer les dispositions du Code de procédure pénale et d'établir un mécanisme juridique efficace pour lutter contre la cybercriminalité, notamment :

- en conférant aux chefs de l'unité opérationnelle, à l'enquêteur et au procureur l'autorité de donner des instructions obligatoires aux propriétaires de données informatiques (opérateurs et fournisseurs de télécommunications, autres entités juridiques et personnes physiques) pour la conservation rapide de données informatiques nécessaires à la résolution du crime, pour une durée maximale de quatre-vingt-dix jours ;
- en établissant les prescriptions portant sur la divulgation par les opérateurs et les fournisseurs de télécommunications, à la demande des services de détection et de répression, des informations nécessaires à l'identification des fournisseurs de services et des moyens par lesquels les informations ont été transmises ;
- en mettant en place un mécanisme efficace pour l'utilisation des preuves sous forme électronique (numérique) dans les procédures pénales ;
- en modifiant le Code de procédure pénale, la loi sur les télécommunications et le projet de loi sur les communications électroniques en vue de la mise en place d'un mécanisme juridique permettant de restreindre temporairement l'accès aux informations ou aux données informatiques affichées sur une certaine ressource (service) informatique (identifiée) et de déterminer la procédure de mise en œuvre.

Le 4 février 2020, la Verkhovna Rada a retiré le projet de loi sur les communications électroniques (règlement n° 2264), pour lequel les services de sécurité avaient présenté des commentaires et des propositions par l'intermédiaire de la Commission parlementaire sur la transformation numérique à la fin de 2019.

Le 5 février 2020, un projet de loi portant le même titre (sur les communications électroniques) et présenté par une équipe d'auteurs presque identique a été enregistré à la Verkhovna Rada sous le numéro 3014. Selon une analyse préliminaire, le nouveau

projet ne contient pas non plus de dispositions qui faciliteraient la pleine mise en œuvre de la Convention sur la cybercriminalité.

En 2020, pour faire face aux problèmes actuels dans le domaine de la cybersécurité, les services de sécurité ont appuyé l'introduction d'une initiative législative permettant l'examen de plusieurs projets de loi par la neuvième législature de la Verkhovna Rada. L'adoption de ces projets de loi créera une base juridique pour les services de sécurité, conformément à la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine.

La loi fait notamment une distinction entre les enquêteurs de la police nationale et ceux des services de sécurité lorsqu'ils enquêtent sur des infractions commises avec des ordinateurs, des systèmes, des réseaux informatiques et des réseaux de télécommunications, des ressources informatiques de l'État et des infrastructures d'information critiques. Ces infractions sont aussi passibles de sanctions plus lourdes.

Pour pouvoir exécuter les tâches visant à prévenir, détecter, faire cesser et dénoncer les crimes contre la paix et la sécurité de l'humanité commis dans le cyberespace et mettre en œuvre les mesures de contre-espionnage et d'enquête visant à lutter contre le cyberterrorisme et le cyberespionnage, des modifications doivent être apportées à la loi sur le contre-espionnage dans le but d'élargir les fonctions et les pouvoirs des organes, des subdivisions et des employés des services de sécurité.

En outre, les principes et les directives pour la mise sur pied du système national de protection des infrastructures critiques n'ont pas été entérinés par la loi et il n'existe pas de définition des infrastructures critiques de l'État dans les règlements (la liste des infrastructures critiques et la liste des infrastructures informatiques critiques n'ont pas encore été établies).

En 2019, le Gouvernement a approuvé les prescriptions générales relatives à la cyberprotection des infrastructures critiques (Résolution n° 518 du Conseil des ministres datée du 19 juin 2019). En l'absence d'une liste nationale des infrastructures critiques et d'une liste des infrastructures informatiques critiques (prévues par la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine), ce texte n'a aucune valeur.

Les incertitudes relatives aux infrastructures critiques de l'État compliquent l'exécution des tâches de cybersécurité confiées aux services de sécurité et à d'autres acteurs du domaine de la cybersécurité.

Le 23 décembre 2019, lors d'une réunion sur la cybersécurité et la cyberdéfense de l'Ukraine, y compris dans le domaine des infrastructures critiques, la Commission parlementaire sur la transformation numérique a souligné l'importance de l'élaboration et de l'adoption de la loi sur les infrastructures critiques et leur protection. Elle a également plaidé pour une adoption rapide des actes du Conseil des ministres visant à mettre en œuvre les dispositions de la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine.

Lors de sa réunion du 19 février 2020, la Commission parlementaire a abordé séparément la question de l'application pratique de la loi sur les principes fondamentaux du maintien de la cybersécurité en Ukraine et de l'adoption des règlements nécessaires à sa mise en œuvre.

Les institutions, organisations et entreprises nationales demeurent tributaires de logiciels d'origine étrangère, qui peuvent contenir des failles intentionnelles et des fonctions non documentées. L'absence de règles qui permettraient de réduire cette dépendance critique pose toujours problème.

Selon les spécialistes des services de sécurité, il faut élaborer un programme national de remplacement des importations dans le domaine du numérique et arrêter des mesures pour soutenir les producteurs nationaux de logiciels et mettre en place :

- un registre des fournisseurs de logiciels agréés pour les infrastructures informatiques critiques et une procédure pour leur inscription ou leur radiation du registre en question ;
- un registre des logiciels propriétaires recommandés pour les infrastructures informatiques critiques ;
- un répertoire national des logiciels libres et une mise en œuvre renforcée des programmes de l'État pour le transfert aux autorités et à l'administration publiques de leur utilisation.

En outre, afin de riposter immédiatement et efficacement aux menaces existantes et en puissance qui pèsent sur les intérêts nationaux et sur la sécurité de l'Ukraine dans le domaine des technologies numériques, il convient de modifier la loi sur les sanctions pour y introduire des restrictions sur l'utilisation par les infrastructures critiques de tous types de logiciels propriétaires (y compris les antivirus) et de matériel de télécommunication mis au point ou fabriqué par des entités économiques du pays agresseur.

La législation nationale ne prévoit pas de mécanisme contraignant permettant de bloquer l'accès d'un utilisateur aux ressources d'Internet et de supprimer les messages qui contiennent des informations obtenues illégalement, cette lacune constituant un autre facteur négatif.

Il convient également de signaler que les services de sécurité prennent des mesures de coopération internationale pour le renforcement de la sécurité de l'information et de la cybersécurité. Conformément à la stratégie ukrainienne de cybersécurité, les priorités et domaines d'intervention principaux sont les suivants :

- le renforcement de la coopération internationale dans le domaine de la cybersécurité ;
- le soutien aux initiatives internationales (correspondant aux intérêts nationaux) dans le domaine de la cybersécurité ;
- l'approfondissement de la coopération avec l'Union européenne et l'Organisation du Traité de l'Atlantique Nord aux fins du renforcement des capacités de l'Ukraine en matière de cybersécurité ;
- la participation aux mesures de confiance dans le cyberespace prises sous la houlette de l'OSCE.

Dans leurs domaines de compétence, les services de sécurité participent notamment aux activités de CyberEast, un projet conjoint de l'Union européenne et du Conseil de l'Europe destiné aux pays du Programme de partenariat oriental, qui vise à promouvoir des décisions législatives et politiques permettant de mettre en œuvre les dispositions de la Convention de Budapest sur la cybercriminalité. Le projet est exécuté par la Direction générale du voisinage et des négociations d'élargissement de l'Union européenne, en collaboration avec le Bureau de programme sur la cybercriminalité du Conseil de l'Europe.

Sachant qu'il est important d'informer les partenaires internationaux des dernières réalisations de l'Ukraine dans le domaine de la cybersécurité, ainsi que de l'application de certaines mesures de confiance prises conformément aux décisions n^{os} 1039, 1106 et 1202 du Conseil permanent de l'OSCE et portant sur les technologies numériques et leur utilisation, des représentants des services de sécurité

participent en général aux réunions du Groupe de travail informel de l'OSCE sur le sujet. En outre, en application de la mesure de confiance nº 8 prévue dans la décision 1202, les services de sécurité ont désigné un référent qualifié chargé d'effectuer des contrôles programmés ou des contrôles-surprise des communications.

Les services de sécurité prennent part à un autre projet de l'OSCE, qui a pour objectif principal d'analyser de façon détaillée la structure de gouvernance nationale dans le domaine de la cybersécurité, ainsi que l'application des mesures de confiance dans le domaine du numérique et de la cybersécurité, conformément à la décision 1202.

Par ailleurs, dans le cadre des tâches qui leur ont été confiées, les services de sécurité ont obtenu le matériel nécessaire grâce au soutien du Fonds d'affectation spéciale pour la cybersécurité Ukraine-OTAN, qui a également permis la mise sur pied de leur Centre d'opérations pour la cybersécurité. Les objectifs en sont les suivants :

- la prévention, la détection et la répression des crimes contre la paix et la sécurité de l'humanité commis dans le cyberespace ;
- les mesures de contre-espionnage et d'enquête visant à lutter contre le cyberterrorisme et le cyberespionnage ;
- la vérification de l'état de préparation des infrastructures critiques face à d'éventuels cyberincidents et cyberattaques ;
- la lutte contre la cybercriminalité, dont les conséquences peuvent menacer les intérêts vitaux de l'État ;
- les enquêtes sur les cyberincidents et les cyberattaques prenant pour cible les ressources numériques et les infrastructures informatiques critiques de l'État ;
- la garantie d'une riposte aux atteintes numériques contre la sécurité de l'État.

Autre forme de coopération, les services de sécurité procèdent également à l'échange d'informations sur les menaces, les attaques et les atteintes numériques au moyen d'une plateforme d'échange d'informations sur les logiciels malveillants et les menaces dénommée « Ukrainian Advantage ». Il s'agit d'une plateforme publique de coopération entre les services de sécurité et les infrastructures critiques, d'autres entreprises, institutions et organisations, tous propriétaires confondus, ainsi que des particuliers. Cette coopération vise à améliorer la sécurité des utilisateurs de l'information, des télécommunications et des systèmes numériques placés sous la protection des services en vertu d'un accord ou à tout autre titre.

III. Réponses reçues d'organisations intergouvernementales

Union européenne

[Original : anglais]
[20 mai 2020]

Le cyberespace, et en particulier l'Internet mondial et ouvert, est devenu l'épine dorsale de notre société. Il offre une plateforme qui stimule la connectivité et la croissance économique. L'Union européenne et ses États membres sont favorables à un cyberespace mondial ouvert, stable, sûr et pacifique, dans lequel les droits de l'homme, les libertés fondamentales et le droit international s'appliqueraient intégralement afin d'assurer le bien-être de la société, la croissance économique et l'intégrité de sociétés libres et démocratiques.

Alors qu'Internet est de plus en plus présent dans nos vies, nous sommes confrontés à des difficultés communes au monde physique et au cyberespace. Sur la scène internationale, certains États semblent adhérer à la conception d'un cyberespace étroitement contrôlé par le gouvernement, ce qui suscite des préoccupations quant au respect des droits de l'homme et des libertés fondamentales. La recrudescence des actes de malveillance commis par des acteurs étatiques et non étatiques dans le cyberespace est également source de préoccupations. L'Union européenne et ses États membres ont fréquemment exprimé leur inquiétude quant à ces actes malveillants, qui sapent l'ordre international fondé sur des règles et accroissent les risques de conflits.

a) Efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine

L'Union européenne et ses États membres soutiennent fermement les aspirations ci-dessus exposées en faveur de la création d'un cyberespace libre, stable et sûr passant par la promotion et l'application d'un cadre stratégique pour la prévention des conflits et la stabilité dans le cyberespace, ainsi que par un engagement bilatéral, régional et multipartite. Dans ce contexte, l'Union européenne œuvre à renforcer la résilience mondiale, à favoriser et à promouvoir une vision commune d'un ordre international fondé sur des règles dans le cyberespace et à élaborer et à appliquer des mesures de collaboration pratiques, y compris pour le renforcement de la confiance entre les États. Renforcer la résilience numérique mondiale est un élément crucial pour le maintien de la paix et de la stabilité internationales, puisque cela permet de réduire les risques de conflits et de surmonter les difficultés inhérentes à la numérisation de nos économies et sociétés. La résilience mondiale dans le cyberespace permet d'endiguer la capacité d'éventuels auteurs mal intentionnés d'abuser des technologies numériques. Elle permet également aux États de réagir plus efficacement aux atteintes à la cybersécurité et de s'en relever.

La stratégie de cybersécurité intitulée « Un cyberespace ouvert, sûr et sécurisé »[12] et les documents de politique adoptés ultérieurement et cités ci-dessous constituent le point de vue de l'Union européenne sur la meilleure manière de prévenir les perturbations et les attaques dans le cyberespace et d'y faire face. Ces documents visent à promouvoir les valeurs de l'Union européenne et à garantir les conditions propices à la croissance de l'économie numérique. Certaines mesures ont spécifiquement comme but de renforcer la résilience numérique des systèmes informatiques, de lutter contre la cybercriminalité et de renforcer la politique internationale de l'Union européenne en matière de cybersécurité et de cyberdéfense.

En février 2015, le Conseil de l'Union européenne a mis en exergue, par le biais des Conclusions du Conseil sur la cyberdiplomatie[13], l'importance de l'élaboration et de la mise en œuvre futures d'une approche globale et commune à l'échelle de l'Union européenne en matière de cyberdiplomatie qui vise à promouvoir les droits de l'homme et les valeurs fondamentales de l'Union européenne, à garantir la liberté d'expression, à promouvoir l'égalité entre les hommes et les femmes, à stimuler la croissance économique, à lutter contre la cybercriminalité, à atténuer les menaces pour la cybersécurité, à prévenir les conflits et à assurer la stabilité des relations internationales. L'Union européenne appelle également de ses vœux l'adoption d'un modèle de gouvernance d'Internet associant les différentes parties intéressées ainsi que de mesures de renforcement des cybercapacités dans les pays tiers. Elle insiste en outre sur l'applicabilité du droit international existant dans le domaine de la sécurité

[12] Voir communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé ».

[13] 6122/15, Conclusions du Conseil sur la cyberdiplomatie.

internationale et sur la pertinence des normes de comportement, ainsi que sur l'importance de la gouvernance d'Internet, partie intégrante de l'approche globale et commune de l'Union en matière de cyberdiplomatie.

À la suite de l'examen de la Stratégie de cybersécurité de 2013, l'Union européenne a renforcé plus avant ses mécanismes de cybersécurité et ses capacités, de manière coordonnée et en étroite collaboration avec les États membres et les entités de l'Union concernées, et ce, dans le respect de leurs compétences et responsabilités respectives. En 2017, la communication conjointe intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide »[14] faisait état de l'ampleur du défi et de l'éventail de mesures que l'Union européenne pouvait prendre pour être mieux préparée à faire face aux menaces pour la cybersécurité dont le nombre ne cesse d'augmenter.

Les préoccupations relatives à la multiplication des problèmes de cybersécurité ont poussé l'Union européenne à élaborer un cadre dans lequel s'inscrirait une réponse diplomatique conjointe aux actes de malveillance commis dans le cyberespace : la boîte à outils cyberdiplomatique[15]. La capacité et la volonté des acteurs étatiques et non étatiques d'avoir de plus en plus recours à des actes de malveillance dans le cyberespace pour atteindre leurs objectifs devraient être une source de préoccupation mondiale. Ces agissements peuvent constituer des actes répréhensibles en droit international et avoir des effets déstabilisateurs en cascade qui accroissent les risques de conflits. L'Union européenne et ses États membres sont attachés au règlement pacifique des différends dans le cyberespace. À ce titre, le cadre pour une réponse diplomatique conjointe de l'Union européenne s'inscrit dans l'approche de l'Union en matière de cyberdiplomatie et contribue à la prévention des conflits, à l'atténuation des menaces pour la cybersécurité et à une plus grande stabilité dans les relations internationales. Il encourage la coopération, facilite l'atténuation des menaces imminentes et des risques à long terme et influence le comportement des acteurs mal intentionnés à long terme. Il prévoit également la coordination des mécanismes de gestion de crises de l'Union européenne, y compris le Plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs. L'Union européenne et ses États membres encouragent la communauté internationale à renforcer la coopération internationale en faveur d'un cyberespace mondial ouvert, stable, pacifique et sûr, où les droits de l'homme, les libertés fondamentales et l'état de droit sont pleinement respectés. Ils sont déterminés à poursuivre leurs efforts afin de prévenir, décourager, dissuader et circonscrire les actes de malveillance et entendent renforcer la coopération internationale à cette fin.

Par le biais de sa politique internationale relative au cyberespace, l'Union européenne entend promouvoir le respect de ses valeurs fondamentales, définir des normes de comportement responsable et préconiser l'application du droit international existant dans le cyberespace, tout en apportant une aide aux pays non membres au moyen du renforcement des capacités en matière de cybersécurité et en promouvant la coopération internationale dans le domaine informatique.

---

[14] Voir communication conjointe au Parlement européen et au Conseil. « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide ».

[15] 10474/17, Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (« boîte à outils cyberdiplomatique »).

b) Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Menaces existantes et émergentes

L'Union européenne et ses États membres reconnaissent que le cyberespace offre des possibilités considérables de croissance économique, ainsi que de développement durable inclusif. Toutefois, les récentes avancées dans le cyberespace continuent de s'accompagner de difficultés en constante évolution.

L'Union européenne et ses États membres sont préoccupés par l'essor des comportements malveillants dans le cyberespace, y compris l'utilisation abusive et à des fins malveillantes des technologies numériques, ainsi que par la recrudescence du vol de propriété intellectuelle au moyen des technologies numériques. Ces comportements entravent et menacent la croissance économique, ainsi que l'intégrité, la sécurité et la stabilité de la communauté internationale, et peuvent avoir des conséquences déstabilisatrices en cascade qui peuvent créer des risques supplémentaires de conflits.

Plus récemment, alors que la pandémie de maladie à coronavirus (COVID-19) se poursuit, l'Union européenne et ses États membres ont été témoins de menaces cybernétiques et d'actes de malveillance dans le cyberespace prenant pour cible des services essentiels, y compris le secteur des soins de santé, les États membres de l'Union et leurs partenaires internationaux. Ils condamnent ces actes de malveillance dans le cyberespace et expriment leur appui continu au renforcement de la cyberrésilience mondiale.

Les tentatives visant à entraver le bon fonctionnement des infrastructures critiques sont inacceptables et peuvent mettre en danger des vies. Tous les acteurs devraient s'abstenir de commettre des actes irresponsables et déstabilisateurs dans le cyberespace. L'Union européenne et ses États membres appellent tous les pays à faire preuve de la diligence requise et à prendre les mesures qui s'imposent pour lutter contre les auteurs de tels actes se trouvant sur leur territoire, conformément au droit international et aux rapports consensuels du Groupe d'experts gouvernementaux de l'ONU de 2010, 2013 et 2015. Ils soulignent une fois encore que les États ne devraient pas sciemment permettre que leur territoire soit utilisé pour commettre des actes répréhensibles à l'échelle internationale au moyen des technologies numériques et devraient répondre aux demandes formulées par d'autres États d'atténuer les conséquences d'actes de cybermalveillance émanant de leur territoire.

En outre, comme l'a préconisé le Groupe d'experts gouvernementaux dans ses précédents rapports, étant donné la nature unique des technologies numériques, l'approche adoptée par l'Union européenne pour répondre aux problèmes informatiques dans le contexte de la sécurité internationale doit demeurer technologiquement neutre. Cette approche est conforme au principe selon lequel, comme l'ont reconnu les Nations Unies, le droit international existant s'applique aux domaines émergents, y compris l'utilisation des nouvelles technologies.

L'Union européenne et ses États membres ne peuvent qu'appuyer un développement et une utilisation des technologies, systèmes et services associés au numérique qui se fondent sur le respect du droit international et des normes applicables, en particulier la Charte des Nations Unies, ainsi que sur le droit international humanitaire, les principes qui en découlent et les droits de l'homme.

Applicabilité du droit international aux technologies numériques

L'Union européenne et ses États membres sont profondément attachés à un système multilatéral efficace reposant sur un ordre international fondé sur des règles qui permette de relever les défis actuels et futurs dans le cyberespace.

Un cadre réellement universel de cybersécurité ne peut se fonder que sur le droit international existant, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme. En outre, l'Union européenne et ses États membres réaffirment l'applicabilité du droit international existant à la conduite des États dans le cyberespace, comme en attestent les rapports du Groupe d'experts gouvernementaux de 2010, 2013 et 2015 ainsi que les principes visés aux paragraphes 28 a) à 28 f) du rapport de 2015.

Le droit international, y compris le droit international humanitaire, qui comprend les principes de précaution, d'humanité, de nécessité militaire, de proportionnalité et de distinction, s'applique à la conduite des États dans le cyberespace et constitue un cadre global de protection qui définit les limites légales de leur comportement, y compris en temps de conflit. L'Union européenne souligne qu'elle est convaincue que le droit international ne facilite pas les conflits. À l'inverse, il énonce des règles régissant les opérations militaires afin d'en limiter les répercussions et de protéger les populations civiles en particulier.

De plus, les droits de l'homme et les libertés fondamentales consacrées par les instruments internationaux pertinents doivent être respectés et protégés aussi bien en ligne que hors ligne. L'Union européenne se félicite que le Conseil des droits de l'homme[16] et l'Assemblée générale aient réaffirmé ces principes.

Forts de ce constat, l'Union européenne et ses États membres réitèrent leur appui à un dialogue et une coopération continus afin de forger une vision commune de l'application du droit international existant à l'utilisation des technologies numériques par les États et de contribuer aux efforts visant à faire la lumière sur l'applicabilité du droit international, puisque cela contribuerait au maintien de la paix, à la prévention des conflits et à la stabilité mondiale.

L'Union européenne continue d'appuyer les efforts faits actuellement pour promouvoir l'application du droit international existant dans le cyberespace, y compris en ce qui concerne l'échange d'informations et de bonnes pratiques sur l'application du droit international existant dans le cyberespace. Elle s'engage à continuer de faire rapport sur les observations de ses États membres quant à la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, puisque cela permet de promouvoir la transparence et de mieux comprendre les diverses approches nationales, ce qui est essentiel pour le maintien de la paix et de la stabilité à long terme, et de réduire les risques de conflit découlant d'activités menées dans le cyberespace. Il faudrait mettre davantage l'accent sur la sensibilisation à l'applicabilité du droit international existant en tant que moyen de promouvoir la stabilité et de prévenir les conflits dans le cyberespace.

Normes, règles et principes de comportement responsable des États dans le cyberespace

L'Union européenne et ses États membres encouragent tous les États à s'appuyer sur les travaux entérinés à maintes reprises par l'Assemblée générale, notamment la résolution 70/237, à les faire progresser et à appliquer plus avant les normes et mesures de confiance convenues, qui jouent un rôle fondamental en matière de prévention des conflits.

[16] A/HRC/RES/20/8.

L'Union européenne et ses États membres fonderont leur utilisation des technologies numériques sur le droit international existant et sur le respect et l'application des normes, règles et principes facultatifs de comportement responsable des États dans le cyberespace, qui sont énoncés dans les rapports consécutifs du Groupe d'experts gouvernementaux de 2010, 2013 et 2015. Il conviendrait à l'avenir d'encourager le renforcement de la coopération et de la transparence aux fins du partage de bonnes pratiques, y compris eu égard à la manière dont les normes énoncées par le Groupe d'experts gouvernementaux sont appliquées dans le cadre d'initiatives et de dispositifs ad hoc, y compris au sein d'organisations et d'institutions régionales, afin de contribuer aux travaux de sensibilisation et d'appliquer efficacement les normes convenues de comportement responsable des États.

Mesures de confiance

Élaborer des mécanismes efficaces de coopération et d'interaction entre États dans le cyberespace est une composante cruciale de la prévention des conflits. Les instances régionales se sont révélées être une plateforme pertinente de dialogue et de coopération entre acteurs partageant des préoccupations et des intérêts communs qui permet de relever efficacement les difficultés à l'échelle régionale.

En élaborant et en appliquant des mesures de confiance dans le domaine de la sécurité ainsi que des mesures de coopération et de transparence au sein de l'Organisation pour la coopération et la sécurité en Europe (OSCE), du Forum régional de l'Association des nations d'Asie du Sud-Est (ASEAN), de l'Organisation des États américains et d'autres instances régionales, il sera possible de rendre le comportement des États plus prévisible et d'atténuer les risques d'interprétation erronée, d'escalade et de conflits qui pourraient émaner d'atteintes à la cybersécurité, ce qui contribuera à la stabilité à long terme dans le cyberespace.

Coopération et assistance internationales concernant la sécurité des technologies numériques et le renforcement des capacités dans ce domaine

Afin de prévenir les conflits et d'atténuer les tensions découlant de l'utilisation abusive des technologies numériques, l'Union européenne et ses États membres entendent renforcer la résilience mondiale, en mettant en particulier l'accent sur les pays en développement, afin de relever les défis posés par la numérisation économique et sociétale et afin d'endiguer la capacité d'auteurs mal intentionnés à utiliser les technologies numériques à des fins malveillantes. La résilience accroit la capacité des États à réagir aux cybermenaces et à s'en relever.

L'Union européenne et ses États membres soutiennent un large éventail de programmes et initiatives ciblés visant à aider les pays à renforcer leurs compétences et leur capacité de réagir aux atteintes à la sécurité informatique. Ils sont également favorables aux initiatives appelées à faciliter l'échange de bonnes pratiques, que ce soit par le biais d'interactions directes, de contacts bilatéraux ou de la coopération au sein des instances régionales et multilatérales.

L'Union européenne et ses États membres reconnaissent que promouvoir les capacités protectrices adéquates et des produits, processus et services numériques plus sûrs contribuera à façonner un cyberespace plus sûr et fiable. Ils ont également conscience de la responsabilité de tous les acteurs pertinents d'œuvrer au renforcement des capacités dans ce domaine et encouragent une coopération plus étroite avec les principaux partenaires et organisations à l'échelle internationale afin d'appuyer le renforcement des capacités dans les pays tiers.